OnGuard® 2013

System Administration User Guide

PERPETUAL INNOVATION

LENEL

Lenel OnGuard® 2013 System Administration User Guide, product version 6.6
This guide is item number DOC-200, revision 3.027, August 2012

Copyright © 1995-2012 Lenel Systems International, Inc. Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Lenel Systems International, Inc.

Non-English versions of Lenel documents are offered as a service to our global audiences. We have attempted to provide an accurate translation of the text, but the official text is the English text, and any differences in the translation are not binding and have no legal effect.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that agreement. Lenel and OnGuard are registered trademarks of Lenel Systems International, Inc.

Microsoft, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Integral and FlashPoint are trademarks of Integral Technologies, Inc. Crystal Reports for Windows is a trademark of Crystal Computer Services, Inc. Oracle is a registered trademark of Oracle Corporation. Other product names mentioned in this User Guide may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Portions of this product were created using LEADTOOLS © 1991-2012 LEAD Technologies, Inc. ALL RIGHTS RESERVED.

OnGuard includes ImageStream® Graphic Filters. Copyright © 1991-2012 Inso Corporation. All rights reserved. ImageStream Graphic Filters and ImageStream are registered trademarks of Inso Corporation.

Table of Contents

CHAPTER 1 Introduction to System Administration 49

Conventions Used in this Documentation 49
UL Listed Installations 49
Getting Started 49
Passwords 49
Enable/Disable Strong Password Enforcement 50
Change User Passwords 50
Error Messages 51
Accounts 51
Log In 52
Single Sign-On 53
Directory Accounts 54
Automatic and Manual Single Sign-On 54
Configure Single Sign-On 54
Log In Using Automatic Single Sign-On 54
Log In Using Manual Single Sign-On 55
Troubleshoot Logging In 56
Assigning Directory and Internal Accounts to the User 56
Display Customization Procedures 57
Change or Reset the List Font 57
Change or Reset the Disabled Text Color 57
Log Out of the Application 58

CHAPTER 2 Main Window 59

Menus and Toolbars 59
Application Menu 60
Edit Menu 61
View Menu 61

Administration Menu *62*
Access Control Menu *64*
Monitoring Menu *66*
Video Menu *66*
Additional Hardware Menu *67*
Logical Access Menu *68*
Window Menu *68*
Help Menu *68*
Cardholder Menu *69*
Asset Menu *71*
How to Use the Toolbars 72
Reset the Toolbars to their Default Settings *72*
Display/Hide Text Labels on Toolbar Buttons *72*
Main Window Procedures 73
Display the System Tree *73*
Display the System Tree Menu *76*
Dock/Undock the System Tree *76*
Undock the System Tree *77*
Move the System Tree When it is Docked *78*
Configure Multiple Devices Using the Application Wizards *78*
Data Entry Forms 79

Administration 81

CHAPTER 3 Cardholders Folder *83*

Cardholders Folder Fields 84
Cardholders Folder Procedures 87
Cardholder Search Capabilities *87*
Search for a Cardholder Record *88*
Retrieve the Most Recent Search Results *89*
Change the Cardholders Folder View Options *89*
Keyboard Wedge Settings Window 90
CAC Barcodes *91*
Scanning Barcodes with a Wedge Scanner *91*
Keyboard Wedge Settings Window Procedures 94
Configure a Wedge Scanner *94*
Verify Fingerprint(s) Dialog 96
Fingerprint Verification with PIV Cards *96*
Verify Fingerprint(s) Dialog Procedures 97
Verify Fingerprints from a PIV Card *97*
Import Fingerprints from a PIV Card *97*
Overwrite Facial Image Dialog 97
Overwrite Facial Image Dialog Procedure 98
Cardholder Form 98
Import Cardholder/Visitor Data *99*
Prerequisites *99*
Corex Business Card Scanner *100*

GSC (iCLASS) Card *101*
ID Scan *101*
ID-Check Terminal *101*
PIV Card *102*
TWIC Card *102*
Import Cardholder Data *102*
Cardholder Form Procedures 103
Add a Cardholder Record *103*
Modify a Cardholder Record *103*
Delete a Cardholder Record *104*
Delete a Selected Group of Cardholder Records *104*
Destroy all Cardholder Data *104*
Visitor Form 105
Visitor Form Procedures 105
Import Visitor Data *106*
Add a Visitor Record *106*
Modify a Visitor Record *106*
Delete a Visitor Record *107*
Segments Form 107
Segments Form Procedures 108
Modify a Cardholder's Segment Assignment *108*
Change a Group of Cardholder's Segments *108*
Badge Form 109
Badge Form Procedures 114
Add or Replace a Badge Record *114*
Modify a Badge Record *115*
Modify Badges for a Selected Group of Cardholders *115*
Encoding Prerequisites 116
Encode a Badge *116*
Delete a Badge Record *117*
Access Levels Form 117
Access Levels Form Procedures 118
Assign Access Levels to a Badge *118*
Assign Intrusion Authority to the Cardholder *119*
Assign Activation and Deactivation Dates to Access Levels *120*
Assign Access Levels to a Selected Group of Cardholders *121*
Remove Access Levels From a Selected Group of Cardholders *122*
Modify Access Levels Assignments *122*
NGP User Form 123
NGP User Form Procedures 124
Device Owner Form 124
Device Owner Form Procedures 124
Assign a Cardholder to Own a Device *124*
Precision Access Form 125
Precision Access Form Procedures 125
Assign Precision Access Groups to a Badge *126*
Remove Precision Access Groups From a Badge *126*
Biometrics Form 126

Biometrics Form Procedures 127
Search for a Cardholder's Biometric Record 127
Visits Form 128
Visits Form Procedures 129
Modify a Cardholder's Permission to Have Visitors 129
Assets Form 130
Assets Form Procedures 130
Assign an Asset to a Cardholder 130
Unassign an Asset 130
Modify the Asset Group 131
Directory Accounts Form 131
Directory Accounts Form Procedures 131
Link a Cardholder to a Directory Account 131
Unlink a Directory Account 132
Logical Access Form 133
Logical Access Form (Cardholders Folder) Procedures 133
Guard Tours Form 134
Guard Tours Form Procedures 134
Assign Guard Tour Security Clearance Levels to a Cardholder 134
Reports Form 135
Reports Form Procedures 135
Run a Cardholder Report 135
ILS Authorization Form 136
ILS Authorization Form Procedures 137

CHAPTER 4 Badge Print Preview Window 139

Badge Printing Form 140
Badge Print Preview Window Procedures 141
Preview and Print a Badge 141

CHAPTER 5 Visits Folder 145

Visit Right-Click Menu 146
Menu Options 146
Visits Folder Fields 147
Sign In Visit(s) Window 148
Print Badge(s) Window 149
Visits Folder Procedures 150
Visit Search Capabilities 150
Search for All Visits to a Selected Cardholder 151
Search for All Visits by a Selected Visitor 152
Search for Scheduled, Active or Finished Visits 152
Search for All Visits for a Specific Date or Time 153
Retrieve the Most Recent Visit Search Results 154
Find a Cardholder or Visitor Associated with a Visit 154
Add a Visit Record 154
Modify a Visit Record 157

Delete a Visit Record *158*
Print a Visitor Badge *158*
Sign in a Previously Scheduled Visit and Print a Badge *158*
Sign Out a Visit *159*
Visit Form 159
Select Date(s) Window *160*
Select Time Range Window *161*
Status Search Form 162
Details Form 163
E-mail Form 164
Add Recipient Window *165*
Reports Form 166
Reports Form Procedures 167
Run a Visit Report from the Visits Folder *167*
Select Host Wizard: Search Form 168
Select Host Wizard: Select Form 170
Select Visitor Wizard: Search Form 171
Select Visitor Wizard: Select or Add Form 172
Select Visitor Wizard: Add Form 174
Select Visitor Wizard: Select Form 175
Select Import Source Window *176*

CHAPTER 6 Assets Folder 177

Assets Form 178
Asset Types Form *180*
Subtypes Form *181*
Assets Form Procedures 181
Add an Asset *182*
Modify an Asset *182*
Delete an Asset *182*
Assign a Cardholder to an Asset *182*
Search for an Asset Record *183*
Retrieve the Most Recent Search Results *183*
Add an Asset Type/Subtype *183*
Asset Classes Form 184
Asset Classes Form Procedures 186
Assign Classes to an Asset *186*
Modify an Asset Classes Assignment *186*
Add Asset Groups and Classes *186*
Modify Asset Groups and Classes *187*
Assignments Form 189
Assignments Form Procedures 190
Assign a Cardholder to an Asset *191*
Unassign an Asset *191*
Search for a Cardholder Assigned to an Asset *191*
Reports Form 191

Reports Form Procedures 193
Run an Asset Report 193

CHAPTER 7 Badge Templates Folder 195

Badge Template Form 195
Access Levels Form 197
ILS Authorization Form 198
Badge Template Form Procedures 199
Add a Badge Template 199
Assign a Cardholder to a Badge Template 200
Unassign a Cardholder from a Badge Template 200
Move a Cardholder to a Different Badge Template 200
Issue a New Badge to an Existing Cardholder 201
Bulk Badge Template Configuration Form 201
Add Bulk Badge Templates 202
Bulk Unassign Cardholders from Badge Templates 202
Badge Template Assignment Wizard 203
Badge Template Issue New Badge Wizard 203
Badge Template Move Wizard 203

CHAPTER 8 Reports Folder 205

Report Configuration Form 206
Report View Filter Window 207
Report Configuration Form Procedures 210
Add a Report 210
Modify a Report 210
Delete a Report 210
Filter the Report View 211
Preview and Print a Report 211
Reader Reports Form 211
Reader Reports Form Procedures 214
Run a Reader Report 214
Alarm Panel Reports Form 215
Alarm Panel Reports Form Procedures 217
Run an Alarm Panel Report 217
Anti-Passback Reports Form 218
Anti-Passback Reports Form Procedures 221
Run an Anti-Passback Report 221
Date/Time Reports Form 222
Date/Time Reports Form Procedures 225
Run a Date/Time Report 225
Event Reports Form 226
Event Reports Form Procedures 229
Run an Event Report 229
Alarm Acknowledgment Reports Form 229

Alarm Acknowledgment Reports Form Procedures 232
Run an Alarm Acknowledgment Report 232
Receiver Account Zone Reports Form 233
Receiver Account Zone Reports Form Procedures 235
Run a Receiver Account Zone Report 236

CHAPTER 9 Print Report Options Window 237

Print Report Options Window 237
Print a Report 238

CHAPTER 10 Report Print Preview Window 241

Report Print Preview Window 242
Report Print Preview Window Procedures 243
Preview and Print a Report 244
Search a Report for Specific Information 245

CHAPTER 11 Card Formats Folder 247

Card Format Form - Common Fields 247
Magnetic Card Format Form 248
Add a Magnetic Card Format 251
Wiegand Card Format Form 252
Wiegand Card Format Form (ILS) 254
Add a Wiegand Card Format 257
Standard 26-Bit Wiegand Card Formats 258
Determine the Facility Code 259
Standard 75-Bit PIV Card Formats 259
CMS Card Format Form 260
CMS Card Format Form Procedures 260
Credential Agent Card Format Form 261
Add a Credential Agent Smart Card Format 261
GSC (iCLASS) Card Format Form 262
Add a GSC (iCLASS) Smart Card Format 263
HandKey (iCLASS) Card Format Form 264
Add a HandKey (iCLASS) Card Format 265
HandKey (MIFARE) Card Format Form 266
Add a HandKey (MIFARE) Card Format 267
HID Access Control (iCLASS) Card Format Form 267
Application License - HID Access Control (iCLASS) 269
Add an HID Access Control (iCLASS) Smart Card Format 269
Create an HID Access Control (iCLASS) Reader Configuration Card 270
HID Access Control (MIFARE) Card Format Form 270
Application License - HID Access Control (MIFARE) 271
Add an HID Access Control (MIFARE) Smart Card Format 271
Create an HID Access Control (MIFARE) Reader Configuration Card 272

SmartID (MIFARE) Card Format Form 272
Application License - SmartID (MIFARE) *274*
Add a SmartID (MIFARE) Smart Card Format *274*
Create a SmartID (MIFARE) Reader Configuration Card *275*
Lenel (iCLASS) Card Format Form 275
Add a Lenel (iCLASS) Smart Card Format *276*
Lenel (MIFARE) Card Format Form 277
Add a Lenel (MIFARE) Smart Card Format *277*
Smart Card CSN Card Format 278
Add a Smart Card CSN Card Format *279*
IrisAccess (iCLASS) Card Format Form 279
Key Management Window *281*
Add an IrisAccess (iCLASS) Smart Card Format *282*
Modify the Encryption Method or Key *282*
Open Encoding Standard (MIFARE) Card Format Form 283
Add an Open Encoding Standard (MIFARE) Smart Card Format *284*
Create an Open Encoding Standard Key Card *284*
DESFire (TWIC 1.02 Data Model) Card Format Form 284
Add a DESFire (TWIC 1.02 Data Model) Smart Card Format *285*
V-Smart (MIFARE) Card Format Form 286
V-Smart (iCLASS) Card Format Form 288
Application License - Bioscrypt *289*
Add a Bioscrypt Smart Card Format *289*
Segment Membership Form 290
Custom Encoding Prerequisites 291
Custom Encoding Form 291
Database Field Properties Window (Blank) 294
Database Field Properties Window (Date/time) 295
Database Field Properties Window (Text/numeric) 296
Select Decimal ASCII Code Dialog 298
Custom Encoding Procedures 299
Build a Custom Expression: Process Outline *299*
Modify a Custom Expression *299*
Custom Encoding Example 300
Encode the Example Card Format *303*
Card Format Folder Procedures 304
Modify a Card Format *304*
Delete a Card Format *304*

CHAPTER 12 Badge Types Folder 307

Badge Type Form 307
Select Badge Layout Window *308*
Badge Type Form Procedures 311
Add a Badge Type *311*
Modify a Badge Type *312*
Delete a Badge Type *313*
Segment Membership Form 313

Printing Form 314
Printing Form Procedures 316
Modify a Print Setup 316
Encoding Form 316
Encoding Prerequisites 318
Encoding Form Procedures 318
Assign an Encoding Format to a Badge Type 318
Required Fields Form 319
Required Fields Form Procedures 320
Specify Required Fields by Badge Type 320
Badge ID Allocation Form 320
Badge ID Allocation Form Procedures 325
Configure Badge ID Allocation 325
Add a Fixed ID Range 326
Modify a Fixed ID Range 326
Delete a Fixed ID Range 327
Import Badge Information for Cards from a Mapping Table 327
Logical Access Form 328
Logical Access Form Procedures 329
Deactivation Settings Form 329
Use or Lose Badge 329
Badge Deactivate Status 330
Linkage Server 330
Deactivation Settings Form Procedures 331
Configure Use or Lose Badge Settings 331
Configure Badge Deactivate Settings 332
ILS Form 332
ILS Form Procedures 333

CHAPTER 13 Directories Folder 335

Directories Form (General Sub-tab) 335
Directories Form (Authentication Sub-tab) 339
Directories Form (Advanced Sub-tab) 340
Directories Form Procedures 341
Add a Directory 341
Modify a Directory 341
Delete a Directory 342

CHAPTER 14 Users Folder 343

Users Form 343
Users Form Common Fields 344
Users Form (General Sub-tab) 345
Users Form (Directory Accounts Sub-tab) 346
Users Form (Internal Account Sub-tab) 346
Users Form (Permission Groups Sub-tab) 347

Users Form (Segment Access Sub-tab) *348*
Users Form (Area Access Manager Levels Sub-tab) *348*
Users Form (Monitor Zone Assignment Sub-tab) *349*
User Form (Replication Sub-tab) *349*
Users Form Procedures 349
Add a User *350*
Assign Access Level(s) to a User *350*
Assign a Monitor Zone to a User *350*
Link a User Account to a Directory Account *351*
Unlink a User Account from a Directory Account *352*
Restrict User Access to Segments *352*
Modify User Information *353*
Disable a User Account *353*
Hide or Show Disabled User Accounts *353*
Delete a User *353*
Search Form 354
Search Form - Permission Groups Search Mode *355*
Search Form - Selected Permissions AND/OR Search Modes *356*
Permission Groups Tree 356
Configure User Permissions *356*
Keyboard Commands *359*
Permission Dependencies *360*
Compare One Permission Group to Another *360*
Verify Permission Changes Using the Compare Function *360*
System Permission Groups Form 361
System Permission Groups Tree *362*
System Permission Groups Form Procedures 362
Add a System Permission Group *363*
Modify a System Permission Group *363*
Delete a System Permission Group *363*
Cardholder Permission Groups Form 364
Cardholder Permission Groups Tree *365*
Cardholder Permission Groups Form Procedures 366
Add a Cardholder Permission Group *366*
Modify a Cardholder Permission Group *366*
Delete a Cardholder Permission Group *366*
Monitor Permission Groups Form 366
Monitor Permission Groups Form (Permissions Sub-tab) *367*
Monitor Permission Groups Tree *368*
Monitor Permission Groups Form (Control Device Groups Sub-tab) *369*
Monitor Permission Groups Form Procedures 370
Add a Monitor Permission Group *370*
Modify a Monitor Permission Group *370*
Delete a Monitor Permission Group *370*
Report Permission Groups Form 371
Report Permission Groups Tree *372*
Report Permission Groups Form Procedures 373
Add a Report Permission Group *373*
Modify a Report Permission Group *373*
Delete a Report Permission Group *373*
Field/Page Permission Groups Form 374

Field/Page Permission Groups Form Procedures 375
Add a Field/Page Viewing Permission Group 375
Modify a Field/Page Viewing Permission Group 376
Delete a Field/Page Viewing Permission Group 376

CHAPTER 15 Workstations Folder 377

Workstations Form 377
Workstations Form (Activity Printer Sub-tab) 378
Workstations Form (CCTV Controller Sub-tab) 379
Workstations Form (Video Capture Device Sub-tab) 380
Workstations Form (Gate Configuration Sub-tab) 381
Workstations Form Procedures 381
Add a Workstation Entry 381
Modify a Workstation Entry 382
Delete a Workstation Entry 382
Encoders/Scanners Form 382
Encoding Prerequisites 383
Encoders/Scanners Form (General Sub-tab) 384
Encoders/Scanners Form (Location Sub-tab) 385
Encoders/Scanners Form (Communications Sub-tab) 385
Encoders/Scanners Form (Encoding Sub-tab) 388
Encoders/Scanners Form Procedures 388
Configure an Inline or Standalone Encoder/Scanner 388
Modify an Encoder/Scanner Entry 389
Delete an Encoder/Scanner Entry 389

CHAPTER 16 System Options Folder 391

General System Options Form 392
Custom Authorization Text Window 395
General System Options Form Procedures 396
Configure the Authorization Warning 396
General Asset Options Form 397
Web Applications Form 397
Hardware Settings Form 398
Anti-Passback Form 400
Biometrics Form 402
Hand Geometry 402
Bioscrypt 403
Biometrics Form Procedures 403
Configure Biometrics 403
User Commands Form 404
Visits Form 406
Visits Form Procedures 407
Configure Default E-mail Recipients 407
Access Levels/Assets Form 408

Access Levels/Assets Form Procedures 409
Enable Extended Options for Access Levels 409
Runaway Detection Form 409
Controller Encryption Form 410
Master Key Entry Window 413
Controller Encryption Form Procedures 414
Configure Automatic Encryption and Set Keys 414
Configure Manual Encryption and Set Keys 415
Modify Master Keys 416
Export Master Keys 416
Activate Master Keys 416
Client Update Form 416
Client Update Form Procedures 418
Enable and Configure Automatic Client Updates 418
Client Update Troubleshooting 418
Running a Client Update Report 419
ILS Form 419
ILS Form Procedures 421

CHAPTER 17 Cardholder Options Folder 423

General Cardholder Options Form 423
Badge ID Allocation Form - ID Allocation Sub-tab 427
Badge ID Allocation Form - ID Ranges Sub-tab 429
Visits Form 431
Logical Access Form 434
Cardholder Search Results Lists Form 434
Visitor Search Results Lists Form 436
Visit Search Results Lists Form 437
Visit Notification Fields Form 438
Person E-mail Fields Form 439
Automatic Lookup Form 441
Cardholder Options Folder Procedures 441
Configure Cardholder Options 442
Configure ID Allocation 443
Add a Fixed ID Range 444
Modify a Fixed ID Range 444
Delete a Fixed ID Range 444
Configure System-wide Visit Options 445
Synchronize Active Badges with Active Visits 445
Configure the Cardholder Search Results Lists 447
Configure the Visitor Search Results Lists 448
Configure the Visit Search Results Lists 448
Configure the Visit Notification Fields 449
Modify the Person E-mail Fields 450

CHAPTER 18 Segments Folder 453

Segments Folder Procedures 453
Log Into the Application as a User with Access to All Segments 453
Add Segments to Your Installation 454
Segment Options Form 459
Segment Options Form Procedures 461
Configure an Installation to Use Segmentation 462
Enable Additional Segmentation Features 463
Segments Form (Hardware Settings Sub-tab) 463
Segments Form (Anti-Passback Sub-tab) 465
Segments Form (Biometrics Sub-tab) 466
Biometrics Sub-tab Procedures 467
Configure Biometrics 468
Segments Form (User Command Sub-tab) 469
Segments Form (Visits Sub-tab) 470
Visits Sub-tab Procedures 471
Configure Default E-mail Recipients (Segmented System) 471
Segments Form (Access Levels/Assets Sub-tab) 471
Enable Extended Options for Access Levels/Asset 472
Segments Form (Controller Encryption Sub-tab) 473
Master Key Entry Window 476
Controller Encryption Sub-tab Procedures 477
Configure Automatic Encryption and Set Keys 477
Configure Manual Encryption and Set Keys 477
Modify Master Keys 478
Export Master Keys 478
Activate Master Keys 479
Segment Groups Form 479

CHAPTER 19 List Builder Folder 481

Simple Lists Form 481
Simple Lists Form Procedures 483
Add an Entry to a List 483
Modify an Entry in a List 483
Delete an Entry from a List 483

CHAPTER 20 MobileVerify Folder 485

MobileVerify Overview 485
System Settings Form 486
System Settings Form Procedures 486
Configure the System's Force Protection Setting 486
Gates Form 487
Gates Form Procedures 488
Configure Gates 488

CHAPTER 21 DataConduIT Message Queues Folder 491

DataConduIT Message Queues Form (General Sub-tab) 492
DataConduIT Message Queues Form (Settings Sub-tab) 493
DataConduIT Message Queues Form (Advanced Sub-tab) 494
DataConduIT Message Queues Form Procedures 495
Add DataConduIT Message Queue 495
Modify a DataConduIT Message Queue 496
Delete a DataConduIT Message Queue 496

CHAPTER 22 Text Library Folder 497

Text Library Form 498
Text Library Form Procedures 498
Add a Text Library Entry 498
Modify a Text Library Entry 499
Delete a Text Library Entry 499
Linking to the Text Library Entry 499

CHAPTER 23 Archives Folder 501

Visit Records 502
Record Archive & Restore Processes 503
Archiving Form 503
Archiving Form Procedures 506
Configure Archive Parameters 506
Archive Specific Event Types 506
Archive Database Records 507
Data Integrity 507
Restoring Form 509
Restoring Form Procedures 511
Delete an Archive File From the System 511
Restore Records to the Database 512
Delete Restored Records From the Database 513

CHAPTER 24 Scheduler Folder 515

Scheduler Form 515
Scheduler Form Procedures 516
Add and Schedule an Action 516
Display the Scheduler Right-Click Menu 521
Add and Schedule an Action Using the Scheduler Right-Click Menu 521
Start an Action 521
Stop an Action 521
View Action History 522
View the Current Status of an Action 522
Refresh an Action 522
Refresh all Actions 522
Delete a Scheduled Action using the Scheduler Right-Click Menu 523

Modify a Scheduled Action using the Scheduler Right-Click Menu *523*

CHAPTER 25 Action Group Library Folder *525*

Action Groups Overview 525
Action Group Library Form 526
Action Group Library Form Procedures 526
Add an Action Group *526*
Modify an Action Group *527*
Delete an Action Group *528*

CHAPTER 26 Global Output Devices Folder *529*

Global Output Server Overview 529
SMTP Server Settings Form 530
SMTP Server Settings Form Procedures 531
Configure SMTP Server Settings *531*
Paging Devices Form 532
Paging Devices Form Procedures 533
Add A Paging Device *533*
Modify a Paging Device *534*
Delete a Paging Device *534*
Recipients Form 534
Creating New [Modifying] Recipient Window *535*
Creating New [Modifying] Recipient Address Window *535*
Recipients Form Procedures 537
Add a Recipient *537*
Modify a Recipient *537*
Delete a Recipient *538*

Access Control 539

CHAPTER 27 Access Panels Folder *541*

NGP Form Overview 541
ILS Forms Overview 541
LNL-3300 Form Overview 542
LNL-3300 Form (Location Sub-tab) 542
LNL-3300 Form (Primary Connection Sub-tab) 544
LNL-3300 Form (Secondary Connection Sub-tab) 547
LNL-3300 (Options Sub-tab) 550
LNL-3300 (Diagnostics Sub-tab) 553
LNL-3300 (Notes Sub-tab) 554
LNL-3300 (Encryption Sub-tab) 554

LNL-3300 Form Procedures 555
Add an LNL-3300 Access Panel 555
Modify an LNL-3300 Access Panel 556
Delete an LNL-3300 Access Panel 556
Enable an LNL-3300 Access Panel for Host Encryption 556
Enable an LNL-3300 Access Panel for Downstream Encryption 556
Enter Notes for an Access Panel 557
LNL-2220 Form Overview 558
LNL-2220 Form (Location Sub-tab) 558
LNL-2220 Form (Connection Sub-tab) 560
LNL-2220 (Options Sub-tab) 562
LNL-2220 (Diagnostics Sub-tab) 566
LNL-2220 (Notes Sub-tab) 567
LNL-2220 (Encryption Sub-tab) 567
LNL-2220 Form Procedures 568
Add an LNL-2220 Access Panel 568
Modify an LNL-2220 Access Panel 568
Delete an LNL-2220 Access Panel 569
Enable an LNL-2220 Access Panel for Encryption 569
Enable an LNL-2220 Access Panel for Downstream Encryption 569
Promote an LNL-2220 Access Panel to an LNL-3300 570
Enter Notes for an Access Panel 570
LNL-2210 Form Overview 570
LNL-2210 Form (Location Sub-tab) 571
LNL-2210 Form (Connection Sub-tab) 573
LNL-2210 (Options Sub-tab) 574
LNL-2210 (Diagnostics Sub-tab) 577
LNL-2210 (Notes Sub-tab) 578
LNL-2210 (Encryption Sub-tab) 578
LNL-2210 Form Procedures 579
Add an LNL-2210 Access Panel 579
Modify an LNL-2210 Access Panel 580
Delete an LNL-2210 Access Panel 580
Enable an LNL-2210 Access Panel for Encryption 580
Promote an LNL-2210 Access Panel to anLNL-2220 or LNL-3300 580
Enter Notes for an Access Panel 581
LNL-2000 Form Overview 581
LNL-2000 Form (Location Sub-tab) 581
LNL-2000 Form (Primary Connection Sub-tab) 583
LNL-2000 Form (Secondary Connection Sub-tab) 586
LNL-2000 (Options Sub-tab) 589
LNL-2000 (Diagnostics Sub-tab) 592
LNL-2000 (Notes Sub-tab) 593
LNL-2000 (Encryption Sub-tab) 593
LNL-2000 Form Procedures 594
Add an LNL-2000 Access Panel 594
Modify an LNL-2000 Access Panel 595

Delete an LNL-2000 Access Panel *595*
Enable an LNL-2000 Access Panel for Encryption *595*
Promote an LNL-2000 Access Panel to an LNL-2210, LNL-2220, or LNL-3300 . . . . . *595*
Enter Notes for an Access Panel *596*
LNL-1000 Form Overview 596
LNL-1000 Form (Location Sub-tab) 597
LNL-1000 Form (Connection Sub-tab) 599
LNL-1000 Form (Options Sub-tab) 601
LNL-1000 Form (Diagnostics Sub-tab) 604
LNL-1000 Form (Notes Sub-tab) 605
LNL-1000 Form (Encryption Sub-tab) 605
LNL-1000 Form Procedures 606
Add an LNL-1000 Access Panel *606*
Modify an LNL-1000 Access Panel *607*
Delete an LNL-1000 Access Panel *607*
Enable an LNL-1000 Access Panel for Encryption *607*
Promote an LNL-1000 Access Panel to an LNL-2000, LNL-2210, LNL-2220, or LNL-3300 . . . . . *608*
Enter Notes for an Access Panel *608*
LNL-500 Form Overview 608
LNL-500 Form (Location Sub-tab) 609
LNL-500 Form (Connection Sub-tab) 611
LNL-500 Form (Options Sub-tab) 613
LNL-500 Form (Diagnostics Sub-tab) 616
LNL-500 Form (Notes Sub-tab) 617
LNL-500 Form (Encryption Sub-tab) 617
LNL-500 Form Procedures 618
Add an LNL-500 Access Panel *618*
Modify an LNL-500 Access Panel *619*
Delete an LNL-500 Access Panel *619*
Enable an LNL-500 Access Panel for Encryption *619*
Promote an LNL-500 Access Panel to an LNL-1000, LNL-2000, LNL-2210, LNL-2220, or LNL-3300 *619*
Enter Notes for an Access Panel *620*
HID Form Overview 620
HID Form (Location Sub-tab) 621
HID Form (Connection Sub-tab) 623
HID Form (Card Formats Sub-tab) 624
HID Form (Notes Sub-tab) 624
HID Form Procedures 625
Add an HID Access Panel *625*
Modify an HID Access Panel *625*
Delete an HID Access Panel *625*
Enter Notes for an HID Access Panel *625*
Other Form Overview 626
Other Form (Location Sub-tab) 626
Other Form (Connection Sub-tab) 628
Other Form (Options Sub-tab) 630

Other Form (Notes Sub-tab) 631
Other Form Procedures 631
Add an Other Access Panel 631
Modify an Other Access Panel 631
Delete an Other Access Panel 632
Enter Notes for an Access Panel 632
Threshold Settings in the ACS.INI File for Dialup Panels 632

CHAPTER 28 Readers and Doors Folder 635

General Form 635
Hardware Notes 641
General Form Procedures 642
Add a Reader 642
Modify a Reader 643
Delete a Reader 643
Grouping Form 643
Reader Group List Entries 643
Reader Group Labels 643
Grouping Form Fields 644
Grouping Form Procedures 644
Add Reader Groups 644
Search for Readers by Groups 644
Settings Form 645
Settings Form Procedures 651
Configure Reader Settings 651
Controls Form 651
Controls Form Procedures 655
Configure Reader Controls 655
Aux Inputs Form 656
Aux Inputs Form Procedures 659
Configure Reader Input(s) 659
Aux Outputs Form 659
Aux Outputs Form Procedures 661
Configure Reader Output(s) 661
Configure Strike Follower 662
Anti-Passback Form 666
Anti-Passback Form Procedures 668
Configure Area Anti-Passback 668
Configure Timed Anti-Passback 669
Command Programming Form 669
Command Programming Form Procedures 671
Program Reader Keypad Commands 672
Elevator Hardware Form 672
Elevator Hardware Form Procedures 674
Elevator Control Limits 674
Configure the System for Standard Elevator Control Mode 675
Configure the System for Floor Tracking Elevator Control Mode 676

Add an Alarm Panel for an Elevator Reader *676*
Modify an Alarm Panel *677*
Delete an Alarm Panel *677*
ILS Form 677
ILS Form Procedures 681
ILS Priority One Events Form 681
ILS Priority One Events Form Procedures 682
Notes Form 682
Notes Form Procedures 683
Enter Reader Notes *683*

CHAPTER 29 Alarm Panels Folder 685

Alarm Panels Form 685
Alarm Panels Form Procedures 688
Add an Alarm Panel *688*
Modify an Alarm Panel *688*
Delete an Alarm Panel *688*
Add a Visonic Bus Device *688*
Modify a Visonic Bus Device *689*
Delete a Visonic Bus Device *689*
Alarm Inputs Form 689
Alarm Inputs Form Procedures 693
Add an Alarm Input *693*
Modify an Alarm Input *694*
Delete an Alarm Input *694*
Alarm Outputs Form 694
Alarm Outputs Form Procedures 696
Add an Alarm Output *696*
Modify an Alarm Output *696*
Delete an Alarm Output *696*
Input/Output Local Linkage Form 697
Input/Output Local Linkage Form Procedures 697
Create an Input-to-Output Link *698*

CHAPTER 30 Power Supplies 699

Power Supplies Procedures 700

CHAPTER 31 Dialup Configuration Folder 701

Modem Settings Form 701
Host Modems Supported 703
Modem Procedures For Lenel Access Panels 703
Set Up a Lenel Host Modem *703*
Add a Dialup Modem Record *703*
Connect a Modem to a Lenel Access Panel *704*

Set up a Lenel Access Panel for Dialup Connection *704*

CHAPTER 32 Timezones Folder *705*

Holidays Form 705
Holidays Form Procedures 707
Add a Holiday *707*
Modify a Holiday *708*
Delete a Holiday *708*
Timezones Form 708
Timezone Form Procedures 710
Add a Timezone *710*
Modify a Timezone *710*
Delete a Timezone *711*
Timezone/Reader Modes Form 711
Timezone/Reader Modes Form Procedures 714
Select Modes of Operation for a Reader During a Timezone *714*
Modify a Timezone/Reader Assignment *714*
Remove a Timezone/Reader Assignment *715*
Timezone/Area Modes Form 715
Timezone/Area Modes Form Procedures 717
Select Modes of Operation for an Area During a Timezone *717*
Modify a Timezone/Area Assignment *718*
Remove a Timezone/Area Assignment *718*

CHAPTER 33 Access Levels Folder *719*

Hardware Dependencies: 719
Access Levels Form (Access Sub-tab - View Mode) 720
Access Levels Form (Access Sub-tab - Modify Mode) 720
Access Levels Form (Area Permissions (NGP) Sub-tab) 722
Access Levels Form (Extended Options Sub-tab) 724
Access Levels Form Procedures 725
Add an Access Level *725*
Assign Extended Options to an Access Level *726*
Add an NGP Intrusion Level *726*
Modify an Access Level *726*
Delete an Access Level *726*
Similar Access Levels Form 726
Access Level Additional Segments Form 727
Access Level Additional Segments Form Procedures 728
Modify an Access Level for Additional Segments *728*
Extended Options Form 729
Elevator Control Form 730
Elevator Control Form Procedures 732
Add an Elevator Control Level *733*
Modify an Elevator Control Level *733*
Delete an Elevator Control Level *733*

Access Groups Form 734
Access Groups Form Procedures 735
Add an Access Group *735*
Modify an Access Group *735*
Delete an Access Group *735*
Precision Access Form 735
Precision Access Form Procedures 737
Add a Precision Access Inclusion Group *737*
Modify a Precision Access Inclusion Group *738*
Delete a Precision Access Inclusion Group *738*
Permission Profiles (General Sub-tab) 738
Permission Profiles Form (Schedule-Based Sub-tab) 741

CHAPTER 34 Command Keypad Templates Folder 743

Command Keypad Templates User Permissions 743
Intrusion Authority Levels User Permissions 744
Command Keypad Templates Form (Macro Assignments Sub-tab) 744
Command Keypad Templates Form (User Feedback Sub-tab) 745
Command Keypad Templates Form (Default/Any Mask Group Intrusion Commands Sub-tab) . 746
Macros Form 747
Key Sequence Format *748*
Configuring the Command Keypad 749
Setting up a Command Keypad Template and Associating with a Reader *749*

CHAPTER 35 Areas Folder 753

Mustering Overview 753
Interlock Overview 754
Escorts and Turnstiles *755*
Areas Form (General Sub-tab) 756
Areas Form (Intrusion Detection Sub-tab) 760
Zones Dialog *762*
Areas Form (Arming/Disarming Sub-tab) 764
Areas Form Procedures 767
Add an Area *768*
Modify an Area *768*
Delete an Area *768*
Configure an Interlocked Area *768*
Area Groups Form 769
Add an Area Group *770*
Associated Safe Locations Form 770
Associated Safe Locations Form Procedures 771
Configure an Associated Safe Location *771*
Associated Inside Areas Form 771
Associated Inside Areas Form Procedures 772

Configure an Associated Inside Area *772*
Muster Reporting Form 773
Muster Reporting Form Procedures 774
Configure Muster Reporting *774*
Special Two Man Form 775
Configure Special Two Man *775*

CHAPTER 36 Groups Folder 777

Mask Groups Form Overview 777
Mask Groups Form 778
Intrusion Mask Group Permissions *779*
Groups Folder - Mask Groups Form Fields *779*
Mask Group Function Links Window 782
Mask Groups Form Procedures 783
Add an Alarm Mask Group *783*
Add an Intrusion Mask Group *784*
Modify a Mask Group *785*
Delete a Mask Group *785*
Configure Actions in the Mask Group Function Links Window *785*
Device Groups Form 786
Device Groups Form Procedures 788
Add a Device Group *788*
Modify a Device Group *788*
Delete a Device Group *788*

CHAPTER 37 Local I/O Folder 791

Hardware Dependencies 791
NGP Limitations *791*
Local I/O Function Lists Form 792
Local I/O Function Lists Form Procedures 796
Add a Local I/O Function List *796*
Modify a Local I/O Function List *797*
Delete a Local I/O Function List *797*
Device --> Function Links Form 797
Device --> Function Links Form Procedures 798
Link A Device to a Local I/O Function List *798*
Link Host Form 799
Link Access Panel Form 799
Link Alarm Panel Form 800
Link Reader Form 801
Link Area Form 803

CHAPTER 38 Global I/O Folder 805

Global I/O Overview 805

User Permissions for Global I/O *806*
Global I/O and Alarm Monitoring *806*
Global I/O and Segmentation *806*
How Do Global I/O Linkages Work? *807*
Global I/O Considerations *808*
Global Linkage Form (Global Linkage Sub-tab) 808
Global Linkage Form (Input Event Sub-tab) 809
Input Event Configuration Form 811
Global Linkage Form (Output Action Sub-tab) 812
Global Linkage Form Procedures 813
Add a Global I/O Linkage *814*
Modify a Global I/O Linkage *815*
Delete a Global I/O Linkage *815*
Modify a Global I/O Linkage's Segment *815*
Global I/O Event Correlation 816
Adding a Global I/O Event Correlation *816*

CHAPTER 39 EOL Tables Folder 819

Basic Custom EOL Resistor Tables 819
Advanced Custom EOL Resistor Tables 819
Resistance Values 820
EOL Resistor Tables Form 820
EOL Resistor Tables Form Procedures 823
Add an EOL Resistor Table *823*
Modify an EOL Resistor Table *824*
Delete an EOL Resistor Table *824*

CHAPTER 40 Destination Assurance Folder 825

Destination Assurance on Segmented Systems 825
Destination Assurance Form 826
Destination Assurance Form Procedures 827
Configure Destination Assurance *827*

CHAPTER 41 Selective Cardholder Download 829

Selective Cardholder Download Form 829
Configuring a Selective Cardholder Download *831*
Cardholders Added to Panels "On-Demand" *832*

CHAPTER 42 Elevator Dispatching Configuration Folder 835

Elevator Dispatching Configuration Overview 836
Elevator Dispatching User Permissions *836*
Elevator Dispatching and the Cardholder Badge *836*
Cardholder Badge Form Configuration Instructions *837*

Elevator Dispatching Devices Form (Location Sub-tab) 838
Elevator Dispatching Devices Form (Connection Sub-tab) 839
Elevator Dispatching Devices Form (Secondary Connection Sub-tab) 840
Elevator Dispatching Devices Form (Inter-floor Matrix Sub-tab) 841
Elevator Dispatching Devices Form (Notes Sub-tab) 842
Elevator Dispatching Devices Form Procedures 842
Add an Elevator Dispatching Device 842
Enter Notes 843
Elevator Terminal Form (Terminal Configuration Sub-tab) 844
Elevator Terminal Form (Access Control Configuration Sub-tab) 845
Elevator Terminal Form Procedures 846
Add a Terminal 846

Monitoring 847

CHAPTER 43 Alarm Configuration Folder 849

Alarm Definitions Form (View Mode) 850
Link Summary View Window 850
Alarm Definitions Form (Modify Mode for Normal Events) 851
Alarm Definitions Form (Modify Mode for Parameter-Based Events) 851
Alarm Definitions Form Procedures 855
View Device-Event-Alarm Links 855
Add a Custom Alarm 856
Modify an Alarm Definition Record 857
Delete an Alarm Definition Record 858
Alarm Configuration Form 858
Alarm Configuration Form Procedures 860
Configure an Alarm 860
Priority Form 860
Color Form 861
Priority Form Procedures 862
Define an Alarm Priority Range 862
Modify an Alarm Priority Range 863
Delete an Alarm Priority Range 863
Text Form 863
Text Form Procedures 864
Add a Text Record 864
Modify a Text Record 864
Delete a Text Record 865
Audio Form 865
Audio Form Procedures 866
Add an Audio Clip Record 866
Modify an Audio Clip Record 867
Delete an Audio Clip Record 867
CCTV Instructions Form 867

CCTV Instructions Form Procedures 869
Add a CCTV Instruction Record 869
Modify a CCTV Instruction Record 869
Delete a CCTV Instruction Record 869
Use Control Characters in CCTV Command Strings 869
Messages Form 870
Select Recipient Window 872
Add E-mail /Pager Windows 872
Messages Form Procedures 874
Add an Automatic E-mail Message 874
Add an Automatic Page Message 874
View an Automatic Message 875
Modify an Automatic Message 875
Delete an Automatic Message 875
Acknowledgment Actions Form 875
Acknowledgment Actions Form Procedures 877
Configure Acknowledgment Actions 877
Failure to Acknowledge Form 877
Failure to Acknowledge Form Procedures 878
Configure a Failure to Acknowledge Action 878
ILS Priority One Events Form 879
ILS Priority One Events Form Procedures 880

CHAPTER 44 Monitor Zones Folder 881

Monitor Zones Form 881
Monitor Zones Form Procedures 884
Add a Monitor Zone 884
Modify a Monitor Zone 884
Delete a Monitor Zone 885
Monitor Stations Form 885
Monitor Stations Form Procedures 886
Add a Monitoring Assignment 887
Modify a Monitoring Assignment 887
Delete a Monitoring Assignment 887
Event Routing Form 888
Event Routing Form Procedures 889
Add an Event Routing Group 889
Remove Event and Timezone Pairs From an Event Routing Group 890
Delete an Event Routing Group 890

CHAPTER 45 Guard Tour Folder 891

Guard Tour Overview 891
Tours Form 892
Tours Form (Checkpoints Sub-tab) 893
Tours Form (Checkpoint Actions Sub-tab) 893

Tours Form (Messages Sub-tab) *894*
Tours Form (Monitoring Stations Sub-tab) *894*
Tours Form (Tour Video Sub-tab) *895*
Tours Form Procedures 896
Add a Guard Tour *896*
Assign Checkpoint Actions *898*
Create Messages and Link Them to Checkpoint Events *899*
Assign Monitoring Stations to the Tour *901*
Link Camera Devices to Checkpoints *901*
Add Special Instructions *902*
Tour Groups Form 902
Tour Groups Form Procedures 904
Add a Tour Group *904*
Scheduler Form 905
Scheduler Form Procedures 906
Schedule an Automatic Guard Tour Action *906*

CHAPTER 46 Monitoring Options Folder 907

Default Icon Commands Form 907
Default Icon Commands Form Procedures 908
Configure Commands to Execute by Icon Type *908*

Video 909

CHAPTER 47 Digital Video Folder 911

Digital Video Recorder Overview 911
Virtual Matrix Switcher for LDVR and Third Party Recorders *912*
LDVR-SP *912*
LDVR-SP30 . . . . . *913*
LDVR- 408 . . . . . *914*
LDVR- 444 . . . . . *915*
LNVR *916*
goVision R1 and R1.5 . . . . . *917*
goVision R2 . . . . . *917*
NetDVMS *918*
Video Recorder Failover and Redundancy *920*
Time-Lapse Recording *920*
Integration with Storage Calculator *920*
Video Recorder Form 921
Video Recorder Form Right-Click Menu *922*
Import Cameras Dialog *922*
Video Recorder Form (Connection Sub-tab) 924
LNVR Security and Passwords *925*
Video Recorder Form - Connection Sub-tab Fields *925*
Video Recorder Form (Recording Sub-tab) 926

Video Recorder Form (Archiving/Purging Sub-tab) 927
Video Recorder Form (Capacity Sub-tab) 929
Video Recorder Form (Performance Sub-tab) 931
Video Recorder Form (Failover Sub-tab) 932
Video Recorder Form (Notes Sub-tab) 933
Video Recorder Form Procedures 933
Add LNVR Video Recorders 933
Add LNVR Failover Video Recorders 934
Add goVision Recorders 935
Add LDVR, Generic Video, or Loronix Video Recorders 935
Add NetDVMS Video Recorders 936
Configure Send Video with NetDVMS 937
Import IP Cameras from the Storage Calculator 937
Add Multiple LDVR Cameras 938
Enter Notes for a Video Recorder 938
Camera Form 939
IP Cameras 939
Camera Form - Common Form Elements Fields 939
Camera Form (Communication Sub-tab) 940
Camera Form (Connection Sub-tab) 942
Camera Form (Record Settings Sub-tab) 944
Camera Form (Quality Sub-tab) 946
Camera Form (Video Sub-tab) 947
Rotation for PTZ Cameras 949
Camera Form (Video Sensor Sub-tab) 949
Camera Form (Normal Mode Sub-tab) 951
Camera Time Stamps 953
Camera Form (Event Mode Sub-tab) 953
Event Mode Sub-tab Functions 953
Pre- and Post-roll Considerations for goVision Recorders 955
Camera Form (Audio Sub-tab) 956
Camera Form (In-Camera Storage Sub-tab) 957
Camera Requirements 957
Camera Configuration 957
Software Configuration 958
Camera Form - In-Camera Storage Sub-tab Fields 959
Camera Form (Capacity Sub-tab) 959
Camera Form (RTP Settings Sub-tab) 960
Camera Form (Notes Sub-tab) 961
Camera Form Procedures 962
Configure LNVR Cameras 962
Configure LDVR, Generic Video, or Loronix Cameras 963
Add or Delete NetDVMS or goVision Cameras 965
Capture Video on Event Only 965
Capture Video on Demand 966
Increase Frame Rates During Events 966
Estimate RAM Needed for Pre-roll 966
Configure Motion Detection and Apply Motion Mask to a Camera 967

Configure Time-Lapse Recording for LDVR Cameras *968*
Configure Time-Lapse Recording with Motion Detection for LNVR Cameras *968*
Enter Notes for a Camera *969*
Camera Inputs Form 969
Camera Inputs Form Procedures 970
Add a Camera Input *971*
Modify a Camera Input *971*
Delete a Camera Input *971*
Add a goVision Camera Input *971*
Camera Outputs Form 972
Camera Outputs Form Procedures 973
Add a Camera Output *973*
Modify a Camera Output *973*
Delete a Camera Output *974*
Add a goVision Camera Output *974*
Remote Monitor 974
LNVR Security *976*
Remote Monitor Form Procedures 976
Add a Remote Monitor *976*
Modify a Remote Monitor *976*
Delete a Remote Monitor *976*
Device - Camera Links Form 977
Device - Camera Links Form Procedures 978
Add a Device - Camera Link *978*
Add a Device - Camera Link for a goVision Camera *979*
Modify a Device - Camera Link *979*
Delete a Device - Camera Link *979*
Alarm-Video Configuration Form 980
Assign Recipients Dialog *983*
Double Video on Alarm *983*
Alarm-Video Configuration Form Procedures 984
Configure Video and Alarms *984*
Video Event Text Form 985
Auxiliary Services Form 986
Auxiliary Services Form Procedures 987
Add an External Client Server *987*
Configure Send Video with External Clients *988*
Archive Server Form 988
Archive Server Form Procedures 990
Add an Archive Server *991*
Modify an Archive Server *992*
Delete an Archive Server *992*
Security Form 992
Security Form Procedures 994
Change Network Video Password *994*
Video Processing Form 994
PTZ Tour Server Form 994

CHAPTER 48 Video Processing Form 997

Video Processing Form 998
Video Processing Events 1000
Blind Camera (AI) 1000
Brightness Change 1002
Motion Detection (AI) 1003
Embedded IntelligentVideo Events 1004
Embedded Analytics Configuration Wizard 1004
Embedded Event Configuration Types 1005
Video Processing Form Procedures 1006
Add Event Settings 1006
Import Event Settings 1007
Export Event Settings 1007
Add Embedded Analytics 1007

CHAPTER 49 IntelligentVideo Folder 1009

IntelligentVideo Server Form 1010
Performing a Download to the IntelligentVideo Server 1011
IntelligentVideo Server Form Procedures 1011
Configure an IntelligentVideo Server 1012
IntelligentVideo Events Form 1012
IntelligentVideo Events Form Procedures 1014
Add IntelligentVideo Event Settings 1014
Modify IntelligentVideo Settings 1015
Delete IntelligentVideo Settings 1015
Copy and Paste Event Settings 1016
Import Event Settings 1016
Export Event Settings 1016
Add an IntelligentVideo Solution 1016
IntelligentVideo Application Form 1017
IntelligentAudio Events Form 1018
Audio Level Event 1019
IntelligentAudio Events Form Procedures 1020
Add IntelligentAudio Event Settings 1020
Modify IntelligentAudio Settings 1021
Delete IntelligentAudio Settings 1021

CHAPTER 50 Event Configuration/Search Dialogs 1023

Event Configuration/Search Dialog Menu Options 1024
Event Menu 1024
Player Menu 1025
Event Configuration/Search Dialog Fields 1026
Event Configuration/Search Dialog Procedures 1028
Open the Event Configuration/Search Dialog 1028
Configure Event Properties 1029
Set Region of Interest 1029

Configure Perspective Correction *1030*
Open the Video Channel Configuration Dialog *1031*
Video Channel Configuration Dialog 1032
Video Channel Configuration Dialog Procedures 1033
Configure Video Channel Parameters *1033*

CHAPTER 51 Matrix Switcher Folder 1035

Matrix Switcher Overview 1035
Matrix Switcher Form 1036
Matrix Switcher Form Procedures 1038
Add a Matrix Switcher (Real and Virtual) *1038*
Modify a Matrix Switcher (Real and Virtual) *1038*
Delete a Matrix Switcher (Real and Virtual) *1038*
Matrix Switcher Type Form 1039
Matrix Switcher Type Form Procedures 1040
Add a Matrix Switcher Type *1040*
Modify a Matrix Switcher Type *1040*
Delete a Matrix Switcher Type *1040*
Custom Command Grammar for Matrix-based Systems 1040
Examples: *1041*
Custom Command Grammar for Direct PTZ Systems 1042
“D” Protocol *1042*
Matrix Switcher Variable Designations 1044
ASCII Protocol Example: Pan Left *1045*
Binary (“D” Protocol) Example: Pan Left *1045*

Additional Hardware 1047

CHAPTER 52 Fire Panels Folder 1049

Fire Panels Form (Location Sub-tab) 1050
Fire Panels Form (Connection Sub-tab) 1051
Fire Panels Form (Options Sub-tab) 1052
Fire Panels Form (Notes Sub-tab) 1053
Fire Panels Form (Encryption Sub-tab) 1053
Fire Panels Form Procedures 1054
Add a Fire Panel *1054*
Modify a Fire Panel *1055*
Delete a Fire Panel *1055*
Enable a Fire Panel for Encryption *1055*
Enter Notes for a Panel *1055*
Fire Devices Form 1056
Fire Devices Form Procedures 1057
Add a Fire Device *1057*
Modify a Fire Device *1057*

Delete a Fire Device *1057*
Fire Inputs/Outputs Form 1058
Fire Inputs/Outputs Form Procedures 1059
Add a Fire Input/Output *1059*
Modify a Fire Input/Output *1059*
Delete a Fire Input/Output *1059*

CHAPTER 53 Intercom Devices Folder 1061

Intercom Communication 1061
Ericsson MD110 Intercom System *1061*
Intercom Devices Form (Location Sub-tab) 1062
Intercom Devices Form (Connection Sub-tab) 1063
Intercom Devices Form (Notes Sub-tab) 1064
Intercom Devices Form (Encryption Sub-tab) 1064
Intercom Devices Form Procedures 1065
Add an Intercom Exchange *1065*
Modify an Intercom Exchange *1066*
Delete an Intercom Exchange *1066*
Enable an Intercom Exchange for Encryption *1066*
Enter Notes for an Intercom Exchange *1067*
Intercom Stations Form 1067
Intercom Stations Form Procedures 1068
Add an Intercom Station *1068*
Modify an Intercom Station *1069*
Delete an Intercom Station *1069*
Intercom Functions Form 1069
Intercom Functions Overview *1070*
Intercom Functions Form Procedures 1071
Add an Intercom Function *1071*
Modify an Intercom Function *1071*
Delete an Intercom Function *1071*

CHAPTER 54 Personal Safety Devices Folder 1073

Personal Safety Devices Overview 1073
SLC-5 (SpiderAlert Local Controller) 1074
Bus Devices 1074
Personal Safety Devices Form 1075
Location Sub-tab ***1077***
Connection Sub-tab ***1078***
Notes Sub-tab *1078*
Personal Safety Devices Form Procedures 1079
Add a Personal Safety Panel *1079*
Modify a Personal Safety Panel *1080*
Delete a Personal Safety Panel *1080*
Enable a Personal Safety Panel for Encryption *1080*
Enter Notes for a Panel *1080*

Transmitters Form 1081
Transmitter Form Fields 1082
Transmitters Form Procedures 1084
Add a Transmitter 1084
Modify a Transmitter 1085
Delete a Transmitter 1085
Assign a Transmitter to a Cardholder 1085
Assign a Transmitter to an Asset 1086
Delete a Transmitter's Assignment 1086
Transmitter Inputs Form 1086
Transmitter Inputs Form Procedures 1088
Add a Transmitter Input 1088
Modify a Transmitter Input 1088
Delete a Transmitter Input 1088
Assign a Transmitter Input to an Asset 1088
Device Configuration Form 1088
Device Configuration Form Procedures 1090
Configure a Personal Safety Device 1090

CHAPTER 55 Receivers Folder 1093

Receivers Overview 1093
Receiver Accounts Overview 1094
Communication Paths Used by Receivers 1094
Default Receiver Configuration 1095
Bosch D6600 (Bosch SIA and Bosch 6500): 1095
Lantronix Box Communication Configuration for Receivers 1095
Events Overview 1096
Event Code Mappings Overview 1096
Event Logging and Reporting Overview 1096
Receivers Form 1097
Receivers Form (Location Sub-tab) 1098
Receivers Form (Connection Sub-tab) 1100
Receivers Form (Options Sub-tab) 1101
Receivers Form (Notes Sub-tab) 1102
Receivers Form (Encryption Sub-tab) 1102
Receivers Form Procedures 1103
Add a Receiver 1103
Modify a Receiver 1104
Delete a Receiver 1104
Enable a Receiver for Encryption 1104
Enter Notes for a Receiver 1105
Receiver Accounts Form 1105
Receiver Accounts Form (Details Sub-tab) 1106
Receiver Accounts Form (Options Sub-tab) 1107
Receiver Accounts Form Procedures 1108
Add a Receiver Account 1108
Modify a Receiver Account 1108
Delete a Receiver Account 1109

Receiver Account Groups Form 1109
Receiver Account Groups Form (Details Sub-tab) 1110
Receiver Account Groups Form (Account List Sub-tab) 1111
Receiver Accounts Form Procedures 1111
Add a Receiver Account Group 1111
Modify a Receiver Account Group 1112
Delete a Receiver Account Group 1112
Zones Form 1112
Zones Form Procedures 1114
Add a Zone 1114
Modify a Zone 1114
Delete a Zone 1115
Areas Form 1115
Areas Form Procedures 1117
Add an Area 1117
Modify an Area 1117
Delete an Area 1117
Event Code Templates Form 1118
Event Code Templates Form Procedures 1121
Add a Custom Event Code Template 1121
Modify an Event Code Template 1122
Delete an Event Code Template 1122

CHAPTER 56 Intrusion Detection Devices Folder 1123

Intrusion Panels Form 1123
Intrusion Panels Form (Location Sub-tab) 1124
Intrusion Panels Form (Connection Sub-tab) 1125
Intrusion Panels Form (Connection Sub-tab for Galaxy) 1126
Intrusion Panels Form (Options Sub-tab) 1127
Intrusion Panels Form (Notes Sub-tab) 1128
Intrusion Panels Form (Encryption Sub-tab) 1128
Intrusion Panels Form Procedures 1129
Add an Intrusion Panel 1129
Modify an Intrusion Panel 1130
Modify an Intrusion Panel's Segment 1130
Delete an Intrusion Panel 1131
Enable an Intrusion Panel for Encryption 1131
Enter Notes for a Panel 1131
Zones Form 1132
Maximum Number of Zones 1133
Zones Form Procedures 1133
Configure Intrusion Zones 1134
Onboard Relays Form 1134
Maximum Number of Onboard Relays 1135
Onboard Relays Form Procedures 1135
Configure Onboard Relays 1136
Offboard Relays Form 1136
Maximum Number of Offboard Relays 1137

Offboard Relays Form Procedures 1138
Configure Offboard Relays 1138
Doors Form 1138
Doors Form Procedures 1139
Configure Intrusion Doors 1139
Areas Form 1140
Maximum Number of Areas 1141
Areas Form Procedures 1141
Configure an Area 1141
Panel User Groups Form 1142
Panel User Assignment Wizard: Find Person Form 1143
Panel User Assignment Wizard: Select Person Form 1144
Panel User Assignment Wizard: Select Person Form 1144
Panel User Assignment Wizard: Summary Form 1145
Panel User Groups Form Procedures 1145
Add a Panel User Group 1146
Modify a Panel User Group 1146
Modify a Panel User Group's Segment 1146
Delete a Panel User Group 1147
Guardall PX Config Form 1147
PX Integration Procedures 1148

CHAPTER 57 POS Devices Folder 1149

POS Devices Overview 1149
Using OnGuard with POS Devices 1149
Hardware Setup and Configuration 1150
Storing Transactions 1150
Licenses Required 1150
User Permissions Required 1150
POS Devices Folder 1150
POS Devices Folder - Common Fields 1151
POS Devices Form (Location Sub-tab) 1151
POS Devices Form (Connection Sub-tab) 1152
POS Devices Form (Notes Sub-tab) 1153
POS Devices Form (Encryption Sub-tab) 1153
POS Devices Form Procedures 1154
Configure a POS Device 1154
Enable a POS Device for Encryption 1155
Enter Notes for a POS Device 1155
POS Register Form 1155
POS Register Form Procedures 1156
Associate a POS Register with a POS Device 1156

CHAPTER 58 SNMP Managers Folder 1157

SNMP Managers Form (Location Sub-tab) 1158

SNMP Managers Form (Notes Sub-tab) 1159
SNMP Managers Form Procedures 1159
Add an SNMP Manager 1159
Modify an SNMP Manager 1160
Delete an SNMP Manager 1160
Enter Notes for an SNMP Manager 1161
SNMP Agents Form 1161
SNMP Agents Form Procedures 1162
Add an SNMP Agent 1162
Modify an SNMP Agent 1163
Delete an SNMP Agent 1163
SNMP Management Information Base Form 1163
SNMP Management Information Base Form Procedures 1165
Load the MIB File(s) 1165
Modify an SNMP Management Information Base Variable 1166

CHAPTER 59 DataConduIT Sources Folder 1167

DataConduIT Sources Folder 1167
DataConduIT Source Downstream Devices 1168
Licenses Required 1168
User Permissions Required 1169
DataConduIT Service Permission 1169
Add, Modify, and Delete DataConduIT Sources, Devices, and Sub-Devices 1169
Trace DataConduIT Sources, Devices, and Sub-Devices 1169
DataConduIT Sources Form 1169
DataConduIT Sources Form Procedures 1170
Add a DataConduIT Source 1170
Modify a DataConduIT Source 1171
Delete a DataConduIT Source 1171
DataConduIT Devices Form 1172
DataConduIT Devices Form Procedures 1173
Add a DataConduIT Device 1173
Modify a DataConduIT Device 1173
Delete a DataConduIT Device 1173
DataConduIT Sub-Devices Form 1174
DataConduIT Sub-Devices Form Procedures 1175
Add a DataConduIT Sub-Device 1175
Modify a DataConduIT Sub-Device 1175
Delete a DataConduIT Sub-Device 1175

CHAPTER 60 OPC Connections Folder 1177

OPC Client Functions 1177
OPC Connections Folder 1177
OPC Connections Form 1178
Select OPC Server Window 1180

OPC Connections Form Procedures 1180
Add an OPC Connection 1180
Modify an OPC Connection 1181
Delete an OPC Connection 1181
Test OPC Connection 1181
OPC Sources Form 1182
OPC Sources Form Procedures 1183
Modify OPC Source Name 1183
Delete OPC Source 1183
OnGuard OPC Client Scenario 1183
Displaying Data 1185

Logical Access 1187

CHAPTER 61 CMS Folder 1189

ActivIdentity CMS Form 1189
CMS Folder Procedures 1190

Appendices 1191

APPENDIX A Actions 1193

NGP Actions 1193
General Actions Procedures 1194
Specify the Number of Simultaneous Actions 1194
Open an Action Properties Window 1194
Action Group Properties Window 1196
Action Group Properties Window Procedures 1197
Add an Action Group 1197
Action History/Guard Tour Event Purging Properties Window 1198
Action History/Guard Tour Event Purging Properties Window Procedures 1199
Add an Action History/Guard Tour Event Purging Action 1199
Archive/Purge Database Properties Window 1199
Archive/Purge Database Properties Window Procedures 1200
Add an Archive/Purge Database Action 1200
Arm/Disarm Area Properties Window 1200
Arm/Disarm Area Properties Window Procedures 1202
Add an Arm/Disarm Area Action 1202
Automatic Guard Tour Properties Window 1202
Automatic Guard Tour Properties Window Procedures 1204
Add an Automatic Guard Tour Action 1204
Change Network Video Password Properties Window 1204

Change Network Video Password Properties Window Procedures 1206
Change the Network Video Password 1206
Schedule a One-Time Password Change 1206
Schedule a Recurring Password Change 1206
DataExchange Script Properties Window 1207
DataExchange Script Properties Window Procedures 1207
Add a DataExchange Script Action 1208
Deactivate Badge Properties Window 1208
Deactivate Badge Properties Window Procedures 1209
Add a Deactivate Badge Action 1209
Device Output Properties Window 1209
Device Output Properties Window Procedures 1210
Add a Device Output Action 1210
Device Output Group Properties Window 1211
Device Output Group Properties Window Procedures 1212
Add a Device Output Group Action 1212
Elevator Terminal Allowed Floors Properties Window 1212
Elevator Terminal Allowed Floors Properties Window Procedures 1213
Add an Elevator Terminal Allowed Floors Action 1213
Elevator Terminal Mode Properties Window 1214
Elevator Terminal Mode Properties Window Procedures 1214
Add an Elevator Terminal Mode Action 1214
Execute Function List Properties Window 1215
Execute Function List Properties Window Procedures 1216
Add an Execute Function List Action 1216
Generate Event Properties Window 1216
Elevator Terminal Mode Properties Window Procedures 1217
Add an Elevator Mode Action 1217
Global APB System/Segment Reset Properties Window 1218
Global APB System/Segment Reset Properties Window Procedures 1218
Add a Global APB System/Segment Reset Action 1218
Grant/Deny Popup Properties Window 1219
Grant/Deny Popup Properties Window Procedures 1220
Add a Grant/Deny Popup Action 1220
Intercom Call Properties Window 1220
Intercom Call Properties Window Procedures 1222
Add an Intercom Call Action 1222
ISC Database Download Properties Window 1222
ISC Database Download Properties Window Procedures 1223
Add an ISC Database Download Action 1224
ISC Firmware Download Properties Window 1224
ISC Firmware Download Properties Window Procedures 1225
Add an ISC Firmware Download Action 1225
Moving Badges for APB Areas Properties Window 1225
Moving Badges for APB Areas Properties Window Procedures 1226
Add a Moving Badges for APB Areas Action 1226

Muster Mode Initiation Properties Window 1227
Muster Mode Initiation Properties Window Procedures 1227
Add a Muster Mode Initiation Action 1228
Mask/Unmask Alarm Input Properties Window 1228
Mask/Unmask Alarm Input Properties Window Procedures 1229
Add a Mask/Unmask Alarm Input Action 1229
Mask/Unmask Alarm Input for Group Properties Window 1229
Mask/Unmask Alarm Input for Group Properties Window Procedures 1231
Add a Mask/Unmask Alarm Input for Group Action 1231
Mask (Disarm)/Unmask (Arm) Mask Group Properties Window 1231
Mask (Disarm)/Unmask (Arm) Mask Group Properties Window Procedures 1232
Add a Mask (Disarm)/Unmask (Arm) Mask Group Action 1232
Mask/Unmask Door Properties Window 1233
Mask/Unmask Door Properties Window Procedures 1234
Add a Mask/Unmask Door Action 1234
Mask/Unmask Door Forced Open Properties Window 1234
Mask/Unmask Door Forced Open Properties Window Procedures 1235
Add a Mask/Unmask Door Forced Open Action 1235
Mask/Unmask Door Forced Open for Reader Group Properties Window 1236
Mask/Unmask Door Forced Open for Reader Group Properties Window Procedures 1237
Add a Mask/Unmask Door Forced Open for Reader Group Action 1237
Mask/Unmask Door Held Open Properties Window 1237
Mask/Unmask Door Held Open Properties Window Procedures 1238
Add a Mask/Unmask Door Held Open Action 1239
Mask/Unmask Door Held Open for Reader Group Properties Window 1239
Mask/Unmask Door Held Open for Reader Group Properties Window Procedures 1240
Add a Mask/Unmask Door Held Open for Reader Group Action 1240
Open/Close APB Area Properties Window 1241
Open/Close APB Area Properties Window Procedures 1242
Add an Open/Close APB Area Action 1242
Pulse Open Door Properties Window 1242
Pulse Open Door Properties Window Procedures 1243
Add a Pulse Open Door Action 1243
Pulse Open Door Group Properties Window 1243
Pulse Open Door Group Properties Window Procedures 1244
Add a Pulse Open Door Group Action 1244
Reader Mode Properties Window 1245
Reader Mode Properties Window Procedures 1246
Add a Reader Mode Action 1246
Reader Mode Group Properties Window 1246
Reader Mode Group Properties Window Procedures 1248
Add a Reader Mode Group Action 1248
Reset Use Limit Properties Window 1248
Reset Use Limit Properties Window Procedures 1250
Add a Reset Use Limit Action 1250
Run PTZ Tour Properties Window 1250

Run PTZ Tour Properties Window Procedures 1251
Add a Run PTZ Tour Action 1251
Schedule Report Properties Window 1251
Schedule Report Properties Window Procedures 1253
Add a Schedule Report Action 1253
Request Print Action Flowchart 1254
Select PTZ Preset Properties Window 1255
Select PTZ Preset Properties Window Procedures 1255
Add a Select PTZ Preset Action 1256
Select Video Wall Layout Properties Window 1256
Select Video Wall Layout Properties Window Procedures 1257
Add a Select Video Wall Layout Action 1257
Set Forwarding Station Properties Window 1258
Set Forwarding Station Properties Window Procedures 1259
Add a Set Forwarding Station Action 1259
Sign Out Visitor Properties Window 1259
Sign Out Visitor Properties Window Procedures 1260
Add a Sign Out Visitor Action 1260
Silence Area Properties Window 1261
Silence Area Properties Window Procedures 1261
Add a Silence Area Action 1262
Surveillance IP Camera(s) Firmware Download Properties Window 1262
Surveillance IP Camera (s) Firmware Download Properties Window Procedures 1263
Add a Surveillance IP Camera(s) Firmware Download Action 1263

APPENDIX B Alarm/Event Descriptions 1265

NGP Alarm/Event Descriptions 1331

APPENDIX C Multimedia Capture 1339

Required Licenses and Permissions 1339
Photo Form 1340
General Capture Procedures 1343
Open Multimedia Capture 1343
Load (User or Factory) Default Settings 1344
Export an Image 1344
Chromakey Sub-tab 1345
Chromakey Sub-tab Procedures 1346
Apply Chromakey to an Image 1346
Effects Gallery Sub-tab 1347
Use the Effects Gallery 1348
Image Processing Window 1349
Effects Gallery Sub-tab Procedures 1351
Create an Effect Profile 1352
Modify an Existing Effect Profile 1352

Delete an Effect Profile *1353*
General Settings Sub-tab 1353
General Settings Sub-tab Procedures 1356
Enable Automatic Cropping *1356*
Image Requirements for Automatic Cropping *1357*
Correct Imperfect Eye Detection *1358*
Enable Manual Cropping *1358*
Resize the Crop Window *1358*
Move the Crop Window *1358*
Adjust Image Compression *1359*
Prevent Manual Crop Adjustment *1359*
Signature Settings Sub-tab 1359
Signature Settings Sub-tab Procedures 1360
Record a Signature *1361*
WDM Video Settings Sub-tab 1361
WDM Video Settings Sub-tab Procedures 1362
Configure WDM Video Settings *1363*
Capture an Image Using Live Video *1363*
FlashPoint/MCI Video Settings Sub-tab 1364
FlashPoint/MCI Video I/O Settings Sub-tab 1366
FlashPoint/MCI Video Settings Procedures 1367
Configure FlashPoint/MCI Video Capture Settings *1368*
Use High Resolution Analog Video Capture *1368*
Scanner Settings Sub-tab 1370
Scanner Settings Sub-tab Procedures 1371
Preview and Scan an Image *1371*
Bypass the Preview Scan Step *1372*
Digital Camera Settings Sub-tab 1373
Digital Camera Settings Sub-tab Procedures 1374
Capture Digital Images *1374*
File I/O Settings Sub-tab 1374
File I/O Settings Sub-tab Procedures 1375
Configure Multimedia Capture for File Import *1375*
Import a Supported Image File *1376*
Import a Non-Supported Image File *1376*
Hand Geometry Form 1380
Hand Geometry License and Permissions *1380*
HandKey Functionality 1380
Hand Geometry Procedures 1382
Capture Hand Print Templates *1382*
Verify Hand Print Templates *1382*
Modify Hand Print Templates *1383*
About Fingerprints 1383
Fingerprint Images *1383*
Fingerprint Templates *1383*
How Fingerprint Enrollment and Verification Works *1383*
Fingerprint (Bioscrypt) Form 1383
Fingerprint (Bioscrypt) License and Permissions *1384*
Bioscrypt Functionality *1384*

Fingerprint (Bioscrypt) Procedures 1385
Capture Fingerprint (Bioscrypt) Templates 1385
Verify Fingerprint (Bioscrypt) Templates 1386
Duress Fingerprint (Bioscrypt) Template 1386
Encode Smart Cards with Bioscrypt Templates 1387
OpenCapture Form 1387
OpenCapture Licenses and Permissions 1387
OpenCapture Functionality 1387
Fingerprint Verification 1388
OpenCapture Procedures 1390
Capture Multiple Fingers 1391
Capture Individual Finger 1391
Verify Fingerprint Templates 1391
About Iris Patterns 1392
Iris (IrisAccess 3000) Form 1392
License and Permissions 1392
Functionality 1392
Iris (IrisAccess 3000) Procedures 1395
Capture Tips 1395
Capture IrisAccess Templates 1395
Verify IrisAccess Templates 1396
Encode Smart Cards with IrisAccess Templates and Access Control Information 1396
Iris (IrisAccess iCAM) Form 1397
Capture IrisAccess Templates 1398
Verify IrisAccess Templates 1399
Encode Smart Cards with IrisAccess Templates and Access Control Information 1399

APPENDIX D Reports 1401

Description of Reports 1401

APPENDIX E Segmentation 1411

Segments and Segment Groups 1411
Segment Rules and Multiple Segment Assignments 1412
Segment Users and <All Segments> Assignments 1412
Primary Segments 1413
Advanced Segmentation 1413
Usage Scenarios 1414
Card Format Segmentation 1416
Badge Type Segmentation 1416
Cardholder Segmentation 1417
Visitor Segmentation 1418
Allowing Access Levels to Be Assigned by Users in Other Segments 1418
Choosing Segmentation - Ramifications and Process Flow 1420
Process Outline - New Installations 1420
Process Outline - Existing Installation 1420
Object Segmentation Table 1421

APPENDIX F ASCII Character Chart 1429

ASCII Values 0-127 1429
ASCII Values 128-255 1434

APPENDIX G Special Two-Man Rule 1435

Standard Two-Man Rule Overview 1435
Special Two-Man Rule Overview 1436
Definitions 1437
Special 1-Man Mode 1437
Special 2-Man Mode 1438
Special Two-Man Rule Configuration Instructions 1439
Configure the Access Panels for Special Two-Man Rule 1440
Configure the Areas for Special Two-Man Rule 1440
Configure the Badges for Special Two-Man Rule 1441
Configure the Readers for Special Two-Man Rule 1441
Configure the List Builder for Special Two-Man Rule 1441
Configure the Timezone for Special Two-Man Rule 1442

APPENDIX H Inline Encoding 1443

Modify the Encoding section of ACS.INI 1443
Standard Magnetic Format Attributes 1444
Using Non-Standard Track Configurations 1445
Information Specific to Magicard Card Printer Drivers 1445
Information Specific to DNP Magicard (e.g. Prima 4) Printer Drivers 1446
Information Specific to Fargo/Kodak/JVC Card/Legacy Eltron Card Printer Drivers 1446
JIS II Encoding (Fargo) 1447
Information Specific to DataCard Card Printer Drivers 1449
Information Specific to Zebra (formerly Eltron) Card Printer Drivers 1449
Information specific to NiSCA Card Printer Drivers 1449
Direct Printers with Inline Encoders 1450
Configure a Direct Printer for Inline Encoding 1450

APPENDIX I Integrating ActivIdentity CMS with OnGuard 1453

Referenced ActivIdentity Documents 1454
Terminology 1454
Using ActivIdentity CMS with OnGuard 1455
Licensing Requirements for ActivIdentity CMS 1456
Setting up the OnGuard ActivIdentity CMS Client Computer 1456
Install the OnGuard License 1456
Install ActivClient 1456
Configure ActivIdentity CMS in OnGuard 1457
Verify User Permissions 1457
Add a CMS Connection 1457
Verify Connectivity to the Selected CMS 1458

Configure ActivIdentity Cardholder Options *1458*
Add a CMS Smart Card Format *1459*
Add a Badge Type for CMS *1459*
Configure a Workstation for CMS *1461*
Configure an Encoder for CMS *1461*
Add DataConduIT Sources for ActivIdentity (CMS Plug-in Users Only) *1462*
Badge Operations Using ActivIdentity CMS with OnGuard 1464
Encode/Bind a CMS Card *1464*
Encode/Bind a PIV Card *1465*
Issuance Validation *1466*
Modify Badge Status *1467*
Delete a Badge *1467*
Delete a User or Cardholder *1467*
Manage Lost Badges on Systems Integrated with ActivIdentity CMS *1468*
Revoke a PKI Credential in ActivIdentity CMS *1468*

APPENDIX J Intrusion Command 1469

Intrusion Command Overview 1469
Configure the System/Segment User Commands 1469
Configure the Access Levels 1470
Configure the Reader 1470
Arming and Disarming from the LNL-CK Reader Using Global Permission Control Only . . . 1471
Arming and Disarming from the LNL-CK Reader Using Advanced Permission Control 1471

APPENDIX K Lenel ILS (Integrated Locking Solutions) 1473

ILS Integra Locking System Overview 1475
ILS Integra Form 1475
Integra Offline Form (Location Sub-tab) 1476
Integra Offline Form (Connection Sub-tab) 1477
Integra Offline Form (Operators Sub-tab) 1478
Add Operator Dialog *1478*
Integra Offline Form (Notes Sub-tab) 1480
Configure an ILS Integra Lock System 1480
ILS Integra Lock Processing *1480*
ILS Integra Lock Panel Overview *1481*
Integra Offline Lock Overview *1482*
Download Integra Locks from System Administration *1483*
View Integra Offline Lock Events *1484*
System Options Folder - ILS Form Overview *1485*
ILS Custom Encoding Overview *1486*
ILS Badge Types Overview *1487*
Integra Blocking Cards Overview *1488*
ILS Integra Timezones Overview *1489*
ILS Integra Timezones/Reader Modes Overview *1490*
ILS Cardholder Authorization Assignments Overview *1491*
ILS Badge Templates Overview *1491*

ILS Offline/Wireless Locking Systems Overview 1491
ILS Offline Form 1492
ILS Offline Form (Location Sub-tab) 1492
ILS Offline (Operators Sub-tab) 1493
Add Operator Dialog 1494
ILS Offline Form (Options Sub-tab) 1496
ILS Offline Form (Notes Sub-tab) 1497
Configure an ILS Offline Locking System 1497
ILS Offline Lock Processing 1498
ILS Offline Lock Panel Overview 1498
Add an ILS Offline Access Panel 1498
ILS Offline Lock Overview 1499
Add an ILS Offline Lock 1500
Modify ILS Offline Panel Assignment 1501
Modify ILS Offline Lock Type 1502
Download Panels and Locks Overview 1502
Calculate Maximum Cardholders 1504
Download ILS Offline/Wireless Locks from System Administration 1505
View ILS Offline Lock Events 1506
Upload ILS Offline Lock Events Using the Mobile Configurator 1507
ILS Offline/ILS Wireless Timezones Overview 1508
ILS Timezone/Reader Modes Overview 1509
Select Modes of Operation for ILS Locks during a Timezone 1509
Badge Types Folder - ILS Form 1510
Configure ILS Badge Types 1510
ILS Special Purpose Cards 1511
ILS iCLASS Printing and Encoding Overview 1512
Configure ILS iCLASS Printing and Encoding 1513
ILS Reports Overview 1514
ILS Wireless Form 1514
ILS Wireless Form (Location Sub-tab) 1515
ILS Wireless Form (Connection Sub-tab) 1516
ILS Wireless Form (Notes Sub-tab) 1518
Configure an ILS Wireless Locking System 1518
ILS Wireless Lock Processing 1519
ILS Wireless Lock Panel Overview 1519
Add an ILS Wireless Access Panel 1519
ILS Wireless Lock Overview 1520
Add an ILS Wireless Lock 1520
Modify ILS Wireless Panel Assignment 1522
Modify ILS Wireless Lock Type 1522
System Options Folder - ILS Form Overview 1522
ILS Priority One Events Overview 1523
Configure ILS Priority One Events 1524
Download ILS Wireless Firmware 1524
Monitor ILS Wireless Lock Events 1524

APPENDIX L NGP Access Panel Configuration 1527

NGP/CASI Form (Location Sub-tab) 1527

NGP Form (Primary Connection Sub-tab) 1529
NGP Form (Secondary Connection Sub-tab) 1530
NGP Form (Card Formats Sub-tab) 1531
NGP Form (Options Sub-tab) 1532
NGP Form (Log on/PIN Sub-tab) 1534
NGP Form (Invalid Access Sub-tab) 1535
NGP Form (Power Sub-tab) 1536
NGP Form (Equipment Sub-tab) 1537
NGP Form (Diagnostics Sub-tab) 1539
NGP Form (Capacity Sub-tab) 1540
NGP Form (Encryption Sub-tab) 1541
NGP Form (Intrusion Sub-tab) 1542
NGP Form (SIA/CID Sub-tab) 1543
NGP Form (IP Central Station) 1545
NGP Form (STU Sub-tab) 1547
NGP Form (Slots) 1547
NGP Form (Notes Sub-tab) 1549
NGP Readers Overview 1549
General Form 1550
Grouping Form 1552
LCD Keypad Form 1552
LCD Keypad Areas Form 1554
Settings Form 1555
Door Form 1556
In Reader Form 1559
Out Reader Form 1561
Timing and Alarms Form 1564
Auxiliary Inputs Form 1565
Auxiliary Outputs Form 1567
NGP Procedures 1568
Configure the NGP Network Settings *1568*
Add an NGP Access Panel *1569*
Add a Door/Reader to an NGP Access Panel *1570*
Configure an NGP Reader for Cardholder Time and Attendance Reporting *1571*
Configure the NGP Access Level *1571*
Add an Area to an NGP Access Panel *1572*
Add an Area Group *1573*
Configure an Alarm Panel for an NGP Access Panel *1573*
Change Reader Access Modes in Alarm Monitoring *1574*
NGP Optional Procedures 1575
Add an NGP Power Supply *1575*
Add an NGP User *1575*
Configure NGP Permissions *1576*
Configure Permission Profiles *1576*
Configure Local Antipassback *1577*

Add a Local I/O Function List *1577*
Add a Global I/O Linkage *1577*
NGP References 1578
NGP Transmitted Messages (SIA & Contact-ID) 1579
SIA Level 2 Message Format *1580*
Contact-ID Message Format *1581*
Door Alarms *1581*
Event Message List (Sorted by SIA Code) *1582*
Event Message List (Sorted by CID Code) *1585*

APPENDIX M PX Panel Integration 1589

Step 1: Configure Panel Host Communication 1589
Step 2: Configure Devices in OnGuard 1590
Step 3: Configure PX Panel in OnGuard 1591
Step 4: Configure Global Linkage in OnGuard 1592
Step 5: Download Database to the Panel from OnGuard 1592
Troubleshooting 1592
Trace *1592*
Errors *1593*

Index 1595

CHAPTER 1

Introduction to System Administration

System Administration is used to configure access control and Alarm Monitoring environments, including all access control hardware devices, non-hardware system features, and user permissions.

Conventions Used in this Documentation

- Where a term is defined, the word is represented in *italics*.
- Field names and file names are shown in **bold**.
- Menus and menu choices are shown in ***bold italics***.
- Keyboard keys are represented in angle brackets. For example: <Tab>, <Ctrl>.
- Keyboard key combinations are written in two ways:
  - <Ctrl> + <Z> means hold down the first key, then press the second
  - <Alt>, <C> means press the first key, then press the second
- Window buttons on the screen are represented in square brackets. For example: [OK], [Cancel].

UL Listed Installations

Refer to the UL Listed system's Hardware Installation Guide (DOC-600) for required UL294 and UL1076 features/operation.

Getting Started

Passwords

OnGuard includes strong password enforcement, which checks the user's password against password standards. This functionality is designed to enhance password security if single sign-on is not used. If

single sign-on is used (automatic or manual), OnGuard does not enforce password standards. For more information on single sign-on, refer to Single Sign-On on page 53.

The system's strong password enforcement also checks the Lenel database user's password when logging into applications. Database user passwords apply only to Oracle and SQL databases. For information on changing your database password, refer to the Accounts and Passwords chapter in the Installation Guide.

Password Standards

When creating a strong password keep the following guidelines in mind:

- Passwords cannot be blank.
- Passwords cannot be the same as the user name (e.g. SA, SA).
- Passwords cannot be Lenel keywords.
- Although not required, your password should contain numbers, letters, and symbols. Spaces are also acceptable. (e.g. August 18, 2002).
- OnGuard user passwords are not case-sensitive.
- Database passwords conform to the rules of the specific database being used; passwords in SQL Server and Oracle 11g are case sensitive. Passwords in Oracle 10g and earlier are case-insensitive.
- The maximum value for a strong password is 127 characters. The minimum value is 1.

Notes: For Oracle databases the following account username and passwords are not allowed to be used together:

System and Manager

Internal and Oracle

Sys and Change_On_Install

Enable/Disable Strong Password Enforcement

Strong password enforcement is enabled/disabled in System Administration or ID CredentialCenter. When you install OnGuard, by default strong password enforcement is enabled. When you upgrade, by default strong password enforcement is disabled. To manually enable or disable strong password enforcement:

1. Select ***System Options*** from the ***Administration*** menu.
2. Select the General System Options tab.
3. Click [Modify].
4. Select or deselect the **Enforce strong passwords** checkbox.

Note: If you disable the option to enforce strong passwords, you will continue to receive a message stating your password is weak every time you log into an application until you change your OnGuard password to meet the password standards.

5. Click [OK].

Change User Passwords

You can use this feature only if the **Change Password** checkbox is selected for the System Permission Group specified in your User Profile. The **Change Password** checkbox is located on the

Software Options sub-tab on the System Permission Groups form in the Users folder. For more information, refer to Chapter 14: Users Folder on page 343.

User passwords are checked every time a user logs into any application. After a user logs into an application he/she can change his/her user password.

1. From the ***Application*** menu select ***Change Password***.
2. The Change Password window displays. Enter your old password and new password in the appropriate fields. Refer to the Password Standards on page 50 for guidelines in choosing a secure password.
3. A message confirms that you have successfully changed your password.
4. Click [OK].

Note: If you get a weak password message the next time you log into the application, carefully read the message. It may be telling you that your database password is weak and not your user password. To change your database password, refer to the Accounts and Passwords chapter in the Installation Guide.

Error Messages

Read weak password messages/warnings carefully to avoid confusion about whether your user password or database password is weak.

If you have a weak database password you will receive a warning every time you log into any application, until you change your database password. Although it is not recommended, you can acknowledge the warning and continue working in the application. This table describes the password-related error messages that may be generated and which password you need to correct.

- To correct the database password, refer to the Accounts and Passwords chapter in the Installation Guide.
- To correct the user password, select a password that meets the standards specified in Password Standards on page 50.

Warning message	Password to correct
Database password violations: Your password is a keyword that is not allowed. It is highly recommended that you change your password to meet our minimum password standards.	Database
Your password cannot be blank. Please enter a password.	User
User password violations: Passwords cannot be the same as the user name.	User
Your password is a keyword that is not allowed.	User

Accounts

Anyone who wishes to use OnGuard applications must enter a user name and password in order to access the software. The System Administrator should create a unique account for each user of the

applications. The System Administrator can also, for each user, create a list of permissions, which specifies precisely which screens, fields, and buttons the user can access.

During initial installation of the application, default accounts are created. These include:

User name	Password	Type
sa	sa	system account
admin		sample
user		sample
badge		sample

These are provided as samples. You may change the passwords and use the accounts, or remove them. The exception to this is the system account, SA. By definition this account has permission to do anything in the system. A user with system access has unlimited access to the application. You cannot delete or change the system account except to modify the password, which you are strongly encouraged to do as soon as possible to discourage unauthorized use.

The first time you log into OnGuard to configure the application, you should log in as **SA** and your password should be **SA**.

Log In

This procedure describes how to log in without using single sign-on. For a description of single sign-on, refer to Single Sign-On on page 53. To log in using single sign-on, refer to Configure Single Sign-On on page 54.

1. Click the Start button, select ***Programs*** > ***OnGuard*** version, and then select the desired application.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to the next step. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].

Note: This only occurs when the "DataSourceType=" value in the Database section of the **ACS.INI** file is set to 2.

3. The Log On window displays.
   a. In the **User name** field, type the user name assigned to you. When logging in for the first time, your user name is **SA**.
   b. In the **Password** field, type the password assigned to you. When logging in for the first time, your password is **SA**. Note that the characters you type do not appear in the field. Instead, for each character you type, an "*" displays. This is intended to protect against unauthorized access in the event that someone else can see the screen while you type.

   IMPORTANT: After logging in for the first time, you are strongly encouraged to modify the password for the system account as soon as possible to discourage unauthorized use.

   c. In the **Directory** field, select the directory that you wish to log into. For user accounts not using single sign-on, the default is "<Internal>."

d. Select the **Remember user name and directory** checkbox if you want the values you just entered in the **User name** and **Directory** fields to automatically be selected the next time that you log in.

e. Click [OK].

4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning click [Yes].

Note: This is configured in the **Log on authorization warning** section on the General System Options form in the System Options folder in System Administration or ID CredentialCenter. The actual message may differ depending on whether your system has been configured to display the standard message or a custom message.

5. If segmentation is not enabled, skip this step. If segmentation is enabled:

a. The Select Segment window opens. Select the segment you wish to log into.

b. Click [OK].

Single Sign-On

Single sign-on simply means logging into OnGuard with the same user name and password that you use to log into Windows or logging into OnGuard using an LDAP user name and password for authentication. *LDAP* (Lightweight Directory Access Protocol) is a software protocol that enables you to locate businesses, people, files, and devices without knowing the domain name (network address).

Single sign-on allows scripts using the DataConduIT API to authenticate. These scripts will be run under a Windows account. The account that is making the call to the API can be obtained easily this way, and the script can be restricted to those actions that the user is permitted to perform (using standard OnGuard permissions).

Note: The use of the explicit username and password for directory authentication to Windows is strongly discouraged. It is recommended that you do not store Windows passwords in the OnGuard system, since OnGuard uses reversible encryption and Windows does not. If explicit authentication is required, you should use an account that has view only permission to the directory in question.

It is possible to assign both an internal account and one or more directory accounts to a single user. Assigning both types of accounts increases the flexibility of the system during the authentication process. If the directory service is down or cannot be found from the workstation where the user is logging on, that user can instead use the internal account. Using both types of accounts means that you need to manage the internal account user names and passwords in addition to managing the directory accounts.

IMPORTANT: Allowing a user to log on in multiple ways increases the probability that the user's access to the system could be compromised. It is recommended that you standardize on either internal or directory accounts, but not both.

There are cases where assigning both an internal account and a directory account to a user may make sense. In a system where directory accounts are predominantly used, you may also assign an internal account to a user who needs to access the system from locations where the directory service is unavailable. If internal accounts are predominantly used, you may want to assign a directory account to a user so that the user does not need to enter in a password to log on.

Directory Accounts

To log into OnGuard using single sign-on, a user name, password, and directory are required. A *directory* is a database of network resources, such as printers, software applications, databases, and users. The following directories are supported by OnGuard: Microsoft Active Directory, Microsoft Windows NT 4 Domain, Microsoft Windows Local Accounts, and LDAP.

Automatic and Manual Single Sign-On

When a user account is configured for single sign-on, the user can log into OnGuard automatically or manually.

For example, with automatic single sign-on, users simply start OnGuard and they are automatically logged in under their Windows account and directory.

With manual single sign-on, users must manually enter their Windows or LDAP account information (user name and password). Users also have the option of selecting a different configured directory.

If single sign-on is not used, users manually enter a user name and a password that is different from their Windows or LDAP password. The directory is hard-coded to refer to the internal OnGuard user directory.

Notes: Manual single sign-on can be used with the following directories: Microsoft Active Directory, Microsoft Windows NT 4 Domain, and LDAP.

Automatic single sign-on can be used with every directory supported by OnGuard except LDAP because it doesn't provide all the account information required.

Configure Single Sign-On

By default, user accounts do not use sign-on. To configure single sign-on the System Administrator must add a directory and link a user account to the directory.

Notes: For more information, refer to Add a Directory on page 341.

For more information, refer to Link a User Account to a Directory Account on page 351.

Log In Using Automatic Single Sign-On

Automatic single sign-on is supported with Windows domain accounts.

1. Click the Start button, then select ***Programs > OnGuard*** version, and then select the desired application.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to step 3. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].

Note: This only occurs when the "DataSourceType=" value in the Database section of the ACS.INI file is set to 2.

3. If your Windows account is linked to a user, a message will be displayed that says, "Attempting to automatically log you on using your Windows account. To bypass this, hold down SHIFT." To automatically be logged in, do nothing.

4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning, click [Yes].

Note: This is configured in the Log on authorization warning section on the General System Options form in the System Options folder in System Administration or ID CredentialCenter. The actual message may differ depending on whether your system has been configured to display the standard message or a custom message.

5. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Select Segment window opens. Select the segment you wish to log into.
   b. Click [OK].

Log In Using Manual Single Sign-On

Both users who want to log into OnGuard using an LDAP user name and password for authentication and users who want to log in using a Windows domain account can do so using manual single sign-on.

1. Click the Start button, then select ***Programs*** > ***OnGuard*** version, and then select the desired application.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to step 3. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. If your Windows account is linked to a user, a message will be displayed that says, “Attempting to automatically log you on using your Windows account. To bypass this, hold down SHIFT.”

   To manually login or to login using a different user name and password, hold down the <Shift> key. The Log On window opens.

   a. In the **Directory** field, select the directory that you wish to log into. The default is “<Internal>.”

Note: For a Directory to be listed, it must first be added on the Directories form in the Directories folder, which is displayed by selecting ***Directories*** from the ***Administration*** menu in System Administration or ID CredentialCenter.

   b. In the **User name** field, type the Windows user name assigned to you. Do not enter the domain\user name just enter your user name.
   c. In the **Password** field, type the Windows password assigned to you.

Note: A Windows account that is used for single sign-on in OnGuard must have both a user name and a password.

   d. Select the **Remember user name and directory** checkbox if you want the values you just entered in the **User name** and **Directory** fields to automatically be selected the next time that you log in.
   e. Click [OK].
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning, click [Yes].

Note: This is configured in the Log on authorization warning section on the General System Options form in the System Options folder in System Administration or ID CredentialCenter. The actual message may differ depending on whether your system has been configured to display the standard message or a custom message.

5. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Select Segment window opens. Select the segment you wish to log into.
   b. Click [OK].

Troubleshoot Logging In

If you attempted to log in and were unable to do so, make sure that the following conditions have been met:

- You entered a correct user name/password and specified the correct directory.
- If your system is configured to display an authorization warning, you accepted the terms.
- A valid license is installed.
- You have permission to use the application.
- If you attempted to log in and were unable to do so, make sure the following conditions have been met:
  - You entered the correct user name and password for the selected directory of a user with permission to use the application.
  - If the system is configured to display an authorization warning, then you accepted the terms.
  - Verify your acs.ini file has the correct LicenseServer Host and Port settings. The LS License Server service must be started on the specified Host.
  - Log into the License Administration application to verify a valid license is installed.
  - Software based licenses must be activated.
  - USB and Parallel licenses must have License Key Drivers installed.
  - If using single sign-on, ensure the pc user you are logged in as is linked to an internal OnGuard user through an operational directory.

Assigning Directory and Internal Accounts to the User

It is possible to assign both an internal account and one or more directory accounts to a single user. Assigning both types of accounts increases the flexibility of the system during the authentication process. Meaning, if the directory service is down or cannot be found from the workstation where the user is logging on, then the user can use the internal account instead.

However, using both types of accounts means that you need to manage the internal account user names and passwords in addition to managing the directory accounts. Allowing a user to log on in multiple ways increases the probability that the user's access could be compromised. For that reason, it is recommended that you standardize on either internal or directory accounts, but not both.

There are cases where assigning both an internal account and a directory account to a user may make sense. In a system where directory accounts are predominantly used, you may also assign an internal account to a user who needs to access the system from locations where the directory service is

unavailable. If internal accounts are predominantly used, you may want to assign a directory account to a user for that user's convenience, so that the user does not need to enter in a password to log on.

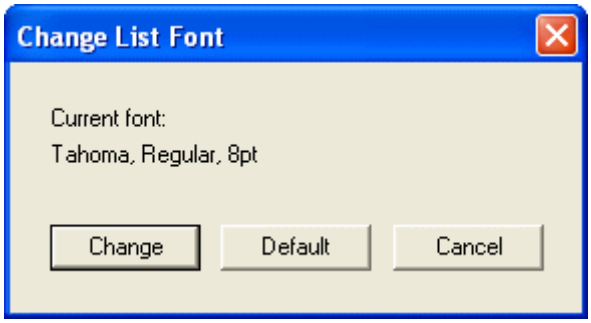
Display Customization Procedures

The following procedures can be used to customize the look of the application.

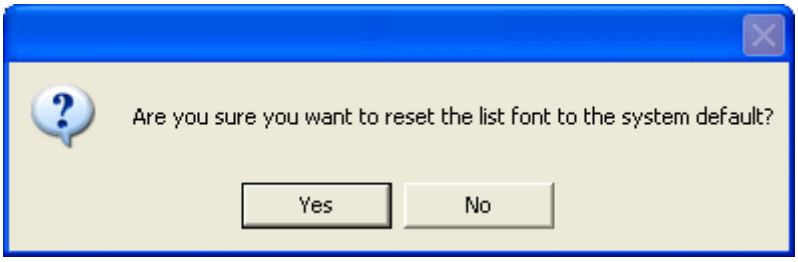
Change or Reset the List Font

The list font is the font used to display text in most listing windows in OnGuard applications. To change the list font, or to reset the list font to the default font:

1. Select ***Change List Font*** from the ***View*** menu.
2. The Change List Font window opens.



- If you wish to change the list font, click [Change]. The Font window opens. Select the font, font style, size, and script you want to use for the list font, then click [OK]. The font will be reset to the system default.
- If you wish to set the list font back to the default setting, click [Default]. Click [Yes] when the following message is displayed:

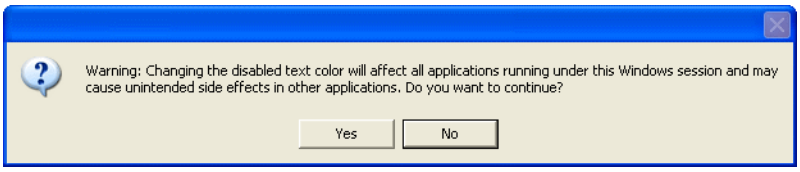


- If you decide not to change the list font, click [Cancel].

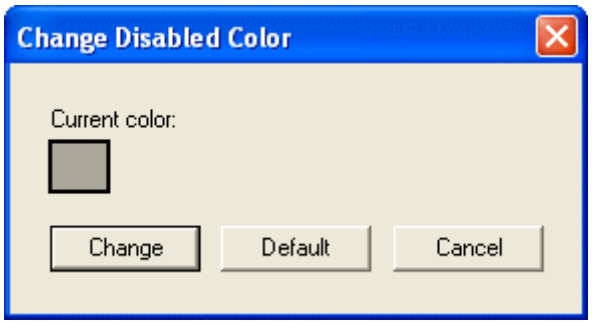
Change or Reset the Disabled Text Color

The disabled text color is the color that text that cannot be changed is displayed in. Typically, this is the “grayed out” text. To change the disabled text color, or to reset the disabled text color to the default color:

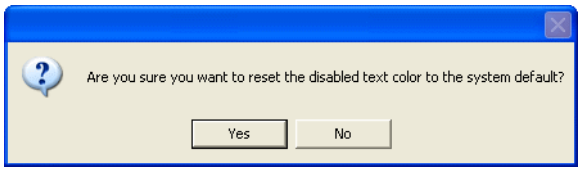
1. Select ***Change Disabled Text Color*** from the ***View*** menu.
2. The following message is displayed. Click [Yes].



3. The Change Disabled Color window opens.



- If you wish to change the disabled text color, click [Change]. The Color window opens. In the Color window, do one of the following:
  - If the color you wish to use is shown in the Basic colors, select it by clicking on it, then click [OK].
  - If the color you wish to use is not shown, you can add a custom color. To do this, click [Define Custom Colors >>]. The window will expand. Click the color palette to select a precise color, or specify the color by entering red, green, blue, hue, saturation, and luminance values. Click [OK].
  - To have a custom color available for future selection, click the [Add to Custom Colors] button after the color is selected.
- If you wish to set the disabled text color back to the default setting, click [Default]. Click [Yes] when the following message is displayed:



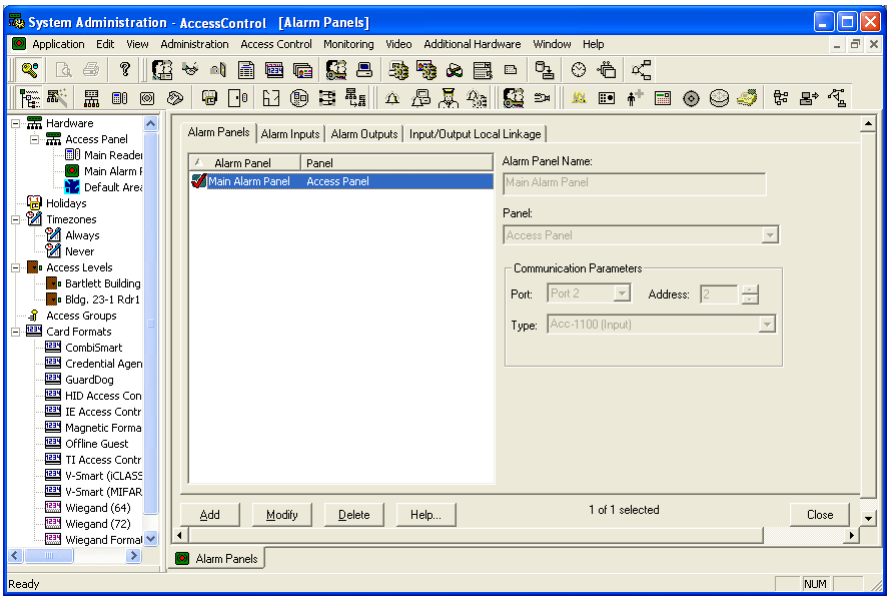
- If you decide not to change the disabled text color, click [Cancel].

Log Out of the Application

1. Select ***Log Off*** from the ***Application*** menu.
2. All open data entry forms will be closed. The main window will open again as it did before you logged in and most of the toolbar and menu options will be dimmed. To access most of the application's features you must then log in again.

CHAPTER 2

Main Window



Menus and Toolbars

The menu bar is a horizontal list of options that appears at the top of the main window. Each option has a pull-down menu.

A toolbar is a strip of buttons that is positioned by default just below the menu bar on the main window. Each button on a toolbar corresponds to a pull-down menu option. You can:

- Change toolbars from anchored to floating

  The toolbars are anchored by default. Anchored toolbars are displayed in horizontal rows below the menu bar. Anchored toolbars can be changed to floating toolbars, which allows the toolbar to be repositioned anywhere in the main window. For more information, refer to How to Use the Toolbars on page 72.

- Control which toolbars are displayed

  Which toolbars are displayed is selected in the ***Toolbars*** sub-menu of the ***View*** menu. By default, all toolbars are displayed. You can control which toolbars are displayed by selecting or deselecting the toolbar entries in this sub-menu. For more information, refer to How to Use the Toolbars on page 72.

- Display text labels on toolbar buttons

  If ***Text Labels*** is selected in the ***Toolbars*** sub-menu of the ***View*** menu, the icons will also contain a descriptive text label. For more information, refer to Display/Hide Text Labels on Toolbar Buttons on page 72.

- Reset toolbars to default values

  The toolbars can be reset to their default values by selecting ***Reset Defaults*** in the ***Toolbars*** sub-menu of the ***View*** menu. For more information, refer to Reset the Toolbars to their Default Settings on page 72.

Application Menu

Wizards

Provides an alternative method to add and configure devices. The button is displayed on the Access Control toolbar.

This option provides wizards that allow you to quickly complete the following tasks:

- Add multiple Lenel readers and ILS offline or wireless locks (up to 32 locks per panel).
- Add multiple Lenel access panels (not available for NGP panels).

Adding downstream devices (off-board readers) to an LNL-2210 panel is not supported if a second on-board reader is configured.

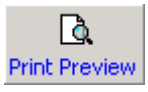
A full panel download may be required the first time downstream devices are added to an LNL-2210 panel that has no downstream devices.

For more information, refer to Configure Multiple Devices Using the Application Wizards on page 78.

Print

Displays the Print Report Options window when a report is selected either on a form in the Reports folder or on the reports form in the Cardholders folder or the Assets folder. The button is displayed on the Main toolbar.

Print Preview



Displays the Report Print Preview window containing the currently selected report. It is only enabled when a report is selected either on a form in the Reports folder or on the reports form in the Cardholders folder or the Assets folder. The button is displayed on the Main toolbar.

Print Setup

Selects a printer and printing options.

Log On

Logs you into the application. The button is displayed on the Main toolbar.

Change Password

Opens the Change Password window, enabling you to change your password (you must have the corresponding system level permission to do so).

Log Off

Logs you out of the application.

Exit

Ends your session.

Edit Menu

Undo

Undoes the last action.

Cut

Removes a selected block of information and places it on the system clipboard.

Copy

Copies a selected block of information and places it on the system clipboard.

Paste

Inserts the contents of the system's clipboard.

Paste Special

Inserts the contents of the system's clipboard, while preserving the formatting.

View Menu

Toolbars

Contains a sub-menu of different toolbars. When a toolbar is selected, that particular toolbar is displayed.

Status Bar

When selected, the status bar is displayed.

Use Tabs in Main Window

When selected, each folder that is opened is displayed on its own tab in the main window. The tab is labeled with the icon and name of the folder. These tabs allow you to navigate quickly between the folders.

Change List Font

Changes the typeface and point size used to display data in listing windows.

Change Disabled Text Color

Allows you to customize the color of data displayed in dimmed fields.

Save Settings On Exit

If selected, most settings that you change will be saved when you logout or exit the application. The settings that change are the size and position of the window, the toolbar setting, the status bar setting, and the tabs setting.

System Tree

Displays the System Tree, a hierarchical listing of system configuration components. The button is displayed on the Access Control toolbar.

View Menu - Toolbar Sub-menu

Reset Defaults

Resets the toolbars displayed to the default settings.

Text Labels

If selected, each toolbar button displays an icon and a descriptive text label. If not selected, only the icon is displayed on the toolbar button.

Main

If selected, the Main toolbar will be displayed on the main window.

Administration

If selected, the Administration toolbar will be displayed on the main window.

Access Control

If selected, the Access Control toolbar will be displayed on the main window.

Monitoring

If selected, the Monitoring toolbar will be displayed on the main window.

Video

If selected, the Video toolbar will be displayed on the main window.

Additional Hardware

If selected, the Additional Hardware toolbar will be displayed on the main window.

Administration Menu

Cardholders

Displays the Cardholders folder of data entry forms. The button is displayed on the Administration toolbar.

Visits

Displays the Visits folder, which contains the Visits data entry form. The button is displayed on the Administration toolbar.

Assets

Displays the Assets folder of data entry forms. The button is displayed on the Administration toolbar.

Reports

Displays the Reports folder of data entry forms. The button is displayed on the Administration toolbar.

Card Formats

Displays the Card Formats folder of data entry forms. The button is displayed on the Administration toolbar.

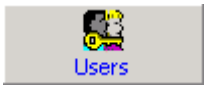
Badge Types

Displays the Badge Types folder of data entry forms. The button is displayed on the Administration toolbar.

Directories

Displays the Directories folder of data entry forms.

Users



Displays the Users folder of data entry forms. The button is displayed on the Administration toolbar.

Workstations

Displays the Workstations folder of data entry forms. The button is displayed on the Administration toolbar.

System Options

Displays the System Options folder of data entry forms. The button is displayed on the Administration toolbar.

Cardholder Options

Displays the Cardholder Options folder of data entry forms. The button is displayed on the Administration toolbar.

Segments

Displays the Segments folder of data entry forms. The button is displayed on the Administration toolbar.

List Builder

Displays the List Builder folder of data entry forms. The button is displayed on the Administration toolbar.

MobileVerify

Displays the MobileVerify folder of data entry forms.

DataConduIT Message Queues

Displays the DataConduIT Message Queues folder of data entry forms.

Archives

Displays the Archives folder of data entry forms. The button is displayed on the Administration toolbar.

Scheduler

Displays the Scheduler folder of data entry forms. The button is displayed on the Administration toolbar.

Action Group Library

Displays the Action Group Library folder of data entry forms. The button is displayed on the Administration toolbar.

Global Output Devices

Displays the Global Output Devices folder of data entry forms. The button is displayed on the Administration toolbar.

Download Entire System

Downloads the entire system to all access panels.

Access Control Menu

Access Panels

Displays the Access Panels folder of data entry forms. The button is displayed on the Access Control toolbar.

Readers

Displays the Readers folder of data entry forms. The button is displayed on the Access Control toolbar.

Alarm Panels

Displays the Alarm Panels folder of data entry forms. The button is displayed on the Access Control toolbar.

Modems

Displays the Dialup Configuration folder of data entry forms. The button is displayed on the Access Control toolbar.

Timezones

Displays the Timezones folder of data entry forms. The button is displayed on the Access Control toolbar.

Access Levels

Displays the Access Levels folder of data entry forms. The button is displayed on the Access Control toolbar.

Areas

Displays the Areas folder of data entry forms. The button is displayed on the Access Control toolbar.

Groups

Displays the Groups folder of data entry forms. The button is displayed on the Access Control toolbar.

Local I/O

Displays the Local I/O folder of data entry forms. The button is displayed on the Access Control toolbar.

Global I/O

Displays the Global I/O folder of data entry forms. The button is displayed on the Access Control toolbar.

EOL Resistor Configuration

Displays the EOL Tables folder of data entry forms.

Destination Assurance

Displays the Destination Assurance folder of data entry forms.

Monitoring Menu

Alarms

Displays the Alarm Configuration folder of data entry forms. The button is displayed on the Monitoring toolbar.

Monitor Zones

Displays the Monitor Zones folder of data entry forms. The button is displayed on the Monitoring toolbar.

Guard Tour

Displays the Guard Tour folder of data entry forms. The button is displayed on the Monitoring toolbar.

Video Menu

Digital Video

Displays the Digital Video folder of data entry forms. The button is displayed on the Video toolbar.

IntelligentVideo

Displays the IntelligentVideo folder of data entry forms. The button is displayed on the Video toolbar.

Matrix Switchers

Displays the Matrix Switcher folder of data entry forms. The button is displayed on the Video toolbar.

Additional Hardware Menu

Fire Panels

Displays the Fire Panels folder of data entry forms. The button is displayed on the Additional Hardware toolbar.

Intercom Devices

Displays the Intercom Devices folder of data entry forms. The button is displayed on the Additional Hardware toolbar.

Personal Safety Devices

Displays the Personal Safety Devices folder of data entry forms. The button is displayed on the Additional Hardware toolbar.

Receivers

Displays the Receivers folder of data entry forms. The button is displayed on the Additional Hardware toolbar.

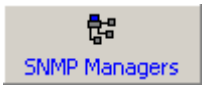
Intrusion Detection Devices

Displays the Intrusion Detection Configuration folder of data entry forms. The button is displayed on the Additional Hardware toolbar.

POS Devices

Displays the POS Devices folder. The button is displayed on the Additional Hardware toolbar.

SNMP Managers



Displays the SNMP Managers folder of data entry forms. The button is displayed on the Additional Hardware toolbar.

DataConduIT Sources

Displays the DataConduIT Sources folder of data entry forms. The button is displayed on the Additional Hardware toolbar.

OPC Connections

Displays the OPC Connections folder of data entry forms. The button is displayed on the Additional Hardware toolbar.

Logical Access Menu

ActivIdentity

Displays the CMS folder of data entry forms, which enables you to configure and test a connection with an ActivIdentity CMS.

Window Menu

Cascade

Places all open forms in an overlapping arrangement.

Tile Horizontally

Places all open forms in a horizontal, nonoverlapping arrangement.

Tile Vertically

Places all open forms in a vertical, nonoverlapping arrangement.

Arrange Icons

Arranges all minimized forms (icons) in a row.

Close All

Closes all open forms (including icons).

[numbered choices]

Lists all forms that are currently open. Select an entry to display that form over (on top of) the other forms.

Help Menu

Contents

Displays online help of the displayed form. The button is displayed on the Main toolbar.

Search

Displays online help table of contents. The button is displayed on the Main toolbar.

Send Feedback

Displays the Send Feedback form. From here you can launch a web feedback form and send feedback directly to Lenel.

About

Displays software version and copyright information.

Cardholder Menu

This menu is only available when a record in the Cardholders folder is displayed

Show Unassigned Assets

If selected, both assets that currently are and assets that once were (but have since been unassigned) assigned to the selected cardholder will be displayed in the listing window on the Assets form. If not selected, only assets that are currently assigned to the selected cardholder will be displayed.

MobileVerify

When selected, displays the MobileVerify Options window where the gate assigned to the current MobileVerify workstation can be changed, or the system's Force Protection Setting can be overridden.

For this option to be available, the following conditions must be met:

- The user must have the MobileVerify Workstation Options permission, which is set on the MobileVerify sub-tab of the System Permission Groups form in the Users folder.
- A recommendation label must have been added to the Cardholder form using FormsDesigner. (The recommendation label may be on a new separate tab or on the Cardholder form.)
- The current workstation must have a gate configuration assigned to it. This is done on the Gate Configuration sub-tab of the Workstations form in the Workstations folder.

Keyboard Wedge Settings

When selected, displays the Wedge Scanner Settings window where you can configure how the OnGuard system interprets the information it receives from a wedge reader. You must have administrative rights to the workstation when setting these options. These settings are set per workstation.

View Options

When selected, displays the View Options window from where you can choose cardholder search attributes.

One Free Pass

If selected, allows the selected cardholder to violate anti-passback rules one time

APB Move Badge

When selected, displays the Area Move Badges window from where you can move a badge to a new area.

Display Global APB Areas

When selected, displays the Cardholder Global APB Areas window. This window lists the global APB areas that the selected cardholder is currently located in.

Show Last Granted Location

If selected, the **Last access** field will display information about the most recent valid access by the selected cardholder, including the triggered event, date, time, and reader name.

Show Last Attempted Location

If selected, the **Last access** field will display information about the most recent access attempt (whether access was granted or not) by the selected cardholder, including the triggered event, date, time, and reader name.

Bulk

Provides a sub-menu of options that can be applied to a select group of cardholder records.

First Record

Displays the first matching cardholder record.

Rewind

Jumps back 10 matching cardholder records.

Previous Record

Displays the previous matching cardholder record.

Next Record

Displays the next matching cardholder record.

Fast Forward

Jumps forward 10 matching cardholder records.

Last Record

Displays the last matching cardholder record.

Cardholder Menu - Bulk Sub-menu

This menu is only available when a record in the Cardholders folder is displayed

Assign Access Levels

Allows you to assign access levels to a select group of cardholder records.

Remove Access Levels

Allows you to remove access levels from a select group of cardholder records.

Modify Badges

If selected, displays the Bulk Modify Badges window from where you can choose to update one or more of the following fields in the Cardholders folder: **Activate Date**, **Deactivate Date**, **Badge Status** and **Use Limit**. You can apply a filter as to which badges you want to update, based on status and/or type. Note that when updating the **Badge Status** field, you must select a badge status filter.

Change Cardholder Segments

When selected, the Bulk Segment Change window opens from where you can change a selected group of cardholder record's segment assignment.

Change Cardholder Replication

When selected, the Change Cardholder Replication window opens from where you can select a new replication setting.

This menu option applies only to Enterprise systems.

Delete Cardholders in Search

Allows you to delete cardholders to a select group of records.

Destroy ALL Cardholder Data

Allows you to destroy all cardholder data.

View Log

When selected, displays the Log Viewer window from where you can view a log of bulk events.

Asset Menu

This menu is only available when a record in the Assets folder is displayed

First Record

Displays the first matching asset record.

Rewind

Jumps back 10 matching asset records.

Previous Record

Displays the previous matching asset record.

Next Record

Displays the next matching asset record.

Fast Forward

Jumps forward 10 matching asset records.

Last Record

Displays the last matching asset record.

Asset Groups and Classes

Displays the Asset Groups and Classes Management window.

Asset Types and Subtypes

Displays the Asset Types and Subtypes Management window.

Show Assignments X Days Past

Displays the Filter Out Assignments After X Days window, which allows you to specify the number of days you want to view.

Bulk Add Mode

Bulk features allow you to add groups of asset records. Selecting bulk Add Mode and entering a value will create a new asset with the same values as the asset that was on the screen when the menu item was selected.

When the Asset folder is first opened this menu item is disabled. The Bulk Add Mode becomes enabled once a search is run.

How to Use the Toolbars

System Administration utilizes standard Windows toolbars.

If you want to:	Do this:
Display the name of a toolbar button.	Point to the toolbar button with the mouse (without clicking).
Use a toolbar button to perform a command or function.	Click the toolbar button with the left mouse button.
Change a toolbar from “anchored” to “floating”.	Double-click on the white vertical bars on the left side of the toolbar you want to move using the left mouse button. white vertical bars →
Change a toolbar from “floating” to “anchored”.	Double-click an empty area of the toolbar.
Rearrange floating toolbars.	1. Click in an empty area of the toolbar. 2. Drag the toolbar to its new position. 3. Release the mouse button to anchor it.
Rearrange anchored toolbars.	1. Click on the white vertical bars on the left side of the toolbar you want to move using the left mouse button. 2. Drag the toolbar to the position on the screen where you want it. 3. Release the mouse button.
To hide or display a toolbar.	1. Choose ***Toolbars*** from the ***View*** menu. A sub-menu displays, containing the name of each toolbar. (A checkmark appears next to each toolbar that is not currently hidden. Toolbars can be toggled in order to be displayed or hidden.) 2. Choose the desired toolbar name.

Reset the Toolbars to their Default Settings

The toolbars can be reset to their original (default) state. In the default state, all six toolbars are displayed in horizontal rows below the menu bar and the toolbar buttons contain only icons.

1. Select the ***View*** menu, point to the ***Toolbars*** menu option, then click ***Reset Defaults***.
2. A message will be displayed that says, “Are you sure you wish to reset to the default toolbar settings?”
3. Click [Yes], and the toolbars will return to their default state.

Display/Hide Text Labels on Toolbar Buttons

By default, each toolbar button contains only an icon. The toolbars can be configured to display a descriptive text label on each button in addition to the icon.

Select the ***View*** menu, point to the ***Toolbars*** menu option, then click ***Text Labels***. This toggles the text labels off and on.

- When the Text Labels menu option is selected (has a checkmark next to it), the toolbar buttons will contain both an icon and a descriptive text label.
- When the Text Labels menu is not selected (has no checkmark next to it), the toolbar buttons will contain only an icon.

Main Window Procedures

Some actions have keyboard shortcuts associated with them. Examples of these include:

Ctrl+N = Add

Ctrl+M = Modify

Delete = Delete

Ctrl+P = Print

Ctrl+Shift+P = Encode

Ctrl+F = Find

Display the System Tree

The System Tree is a sub-window of the main window. The System Tree lists all access control devices defined in System Administration and shows which devices are connected to which other devices. The Window also lists other configuration settings, such as currently defined Timezones and Holidays.

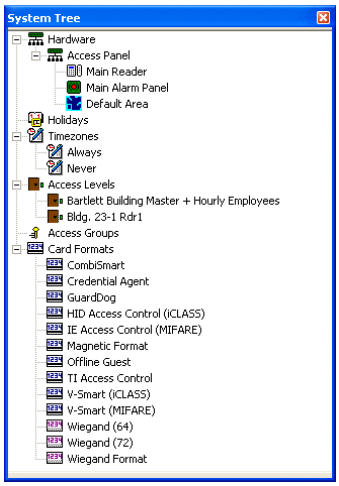
The System Tree is a dockable view that works much like a toolbar (it can be docked and undocked and moved around like a toolbar).

It can be displayed using any of the following methods:

Toolbar Shortcut

- Select the System Tree button on the Access Control toolbar
- <Alt>,<V>,<Y>
- Select ***System Tree*** from the ***View*** menu

The System Tree



The information in the window is displayed in hierarchical fashion, also called a tree or branching arrangement. Each entry in the list contains the name of one device (or, in some instances, one software component such as a timezone). Access Panels have the leftmost entries. For a specific Access Panel, a device connected to it is listed below and indented to the right. Each device connected to those devices is listed below them and further indented. You can search this or any tree by focusing on the list window and clicking “Ctrl+F”. To proceed through the search, press F3 on your keyboard.

Each type of entry is identified by an icon to the left of it. These include:

Icon	Indicates
	Access Control System
	Access Group
	Access Level
	Access Panel
	Alarm Input
	Alarm Mask Group
	Alarm Output
	Alarm Panel
	Area
	Camera
	Card Formats - Magnetic
	Card Formats - Wiegand

Icon	Indicates
	Fire Device
	Fire Input/Output
	Fire Panel
	Function List
	Holiday
	Intercom Exchange
	Intercom Station
	Intrusion Area
	Intrusion Door
	Intrusion Panel
	Intrusion Zone
	Matrix Switcher
	Monitor
	Offboard Relay
	Onboard Relay
	Personal Safety Device
	Reader
	Reader Auxiliary Input
	Reader Auxiliary Output
	Receiver
	Receiver Account
	Segment (only if your system is segmented)
	Timezone

Icon	Indicates
	Video Recorder
	Zone

You can display a popup menu by first clicking with the left mouse button to highlight a window entry, then clicking on the entry using the right mouse button. The menu choices available depend upon the type of entry that is selected.

For most window entries, you can double-click on the entry to display the corresponding data entry form and select that record. For example, double-clicking on an entry opens the Alarm Panels folder, displays the Alarm Inputs form, and selects the corresponding input. This offers a convenient method by which you can accessing a data entry form to review information or make changes. For more information, refer to Data Entry Forms on page 79.

Display the System Tree Menu

To display the System Tree menu:

1. View the System Tree by selecting ***System Tree*** from the ***View*** menu.
2. Right-click on the System Tree.

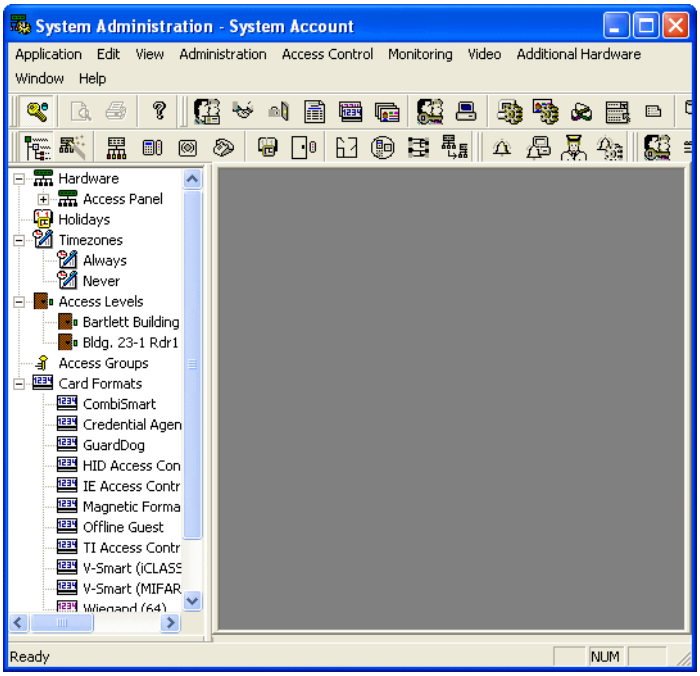
System Tree Menu

Menu option	Function
Find	Acts like a double-click by opening up the related view and selecting the item
Refresh	Refreshes all items from the database
Allow docking	Enables/disables docking of the System Tree view
Hide	Hides the System Tree

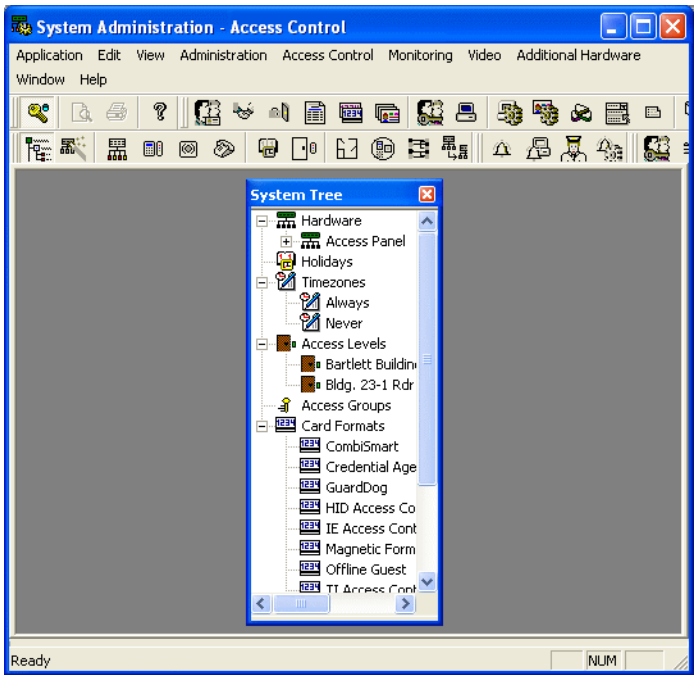
Dock/Undock the System Tree

The System Tree can either float on the screen or be “docked” to one edge of the screen. By default, the System Tree is docked to the left edge of the screen. The two views are shown below:

Docked System Tree View



Undocked System Tree View



Undock the System Tree

1. View the System Tree by selecting ***System Tree*** from the ***View*** menu.
2. Right-click on the System Tree, and the System Tree menu will be displayed. For more information, refer to Display the System Tree Menu on page 76.
3. De-select the ***Allow Docking*** menu option.

- When the ***Allow Docking*** menu option has a checkmark to the left of it, docking of the System Tree IS allowed.
- When the ***Allow Docking*** menu option does not have a checkmark to the left of it, docking of the System Tree is NOT allowed.

If the System Tree has been undocked, you can dock it again by doing the following:

1. Right-click on the System Tree, and the System Tree menu will be displayed. For more information, refer to Display the System Tree Menu on page 76.
2. Select the ***Allow Docking*** menu option.
   - When the ***Allow Docking*** menu option has a checkmark to the left of it, docking of the System Tree IS allowed.
   - When the ***Allow Docking*** menu option does not have a checkmark to the left of it, docking of the System Tree is NOT allowed.
3. Click on the title bar of the System Tree window and drag the System Tree toward the edge of the screen that you want it to dock to. When you are near the edge of the screen, release the mouse button. The System Tree will become “docked” to that side of the screen.

Move the System Tree When it is Docked

Once the System Tree is docked to a side of the screen, the easiest way to dock it to a different edge of the screen is to:

1. Right-click on the System Tree.
2. De-select the ***Allow Docking*** menu option.
3. Right-click again on the System Tree.
4. Select the ***Allow Docking*** menu option.
5. Click on the System Tree’s title bar, drag the System Tree to the new edge of the screen you want it to dock to, and release the mouse.

Configure Multiple Devices Using the Application Wizards

IMPORTANT: Do not use this feature unless you have full knowledge of the hardware.

Use the wizards to rapidly add several panels, readers, and ILS offline or wireless locks and configure their basic settings. The wizards guide you through each step of the process.

In order to run the application wizards, complete the following steps:

1. From System Administration, select the ***Application*** > ***Wizards*** menu. The Wizards window is displayed.
2. Click [Configure access panels] to quickly add and configure multiple Lenel access panels.
3. Click [Configure readers] to quickly add and configure multiple Lenel readers or ILS offline and wireless locks.

Notes: Readers and locks are added per access panel.

Access panels must be added before you can add readers or locks to them.

4. The wizards allow you to configure the common settings of the panels, readers, and locks. However, after you add these devices via the wizard, you will need to complete the process from the Access Control options in System Administration. For example, after configuring readers or

locks in the wizard, configure the remaining lock settings in the Readers and Doors folder as required.

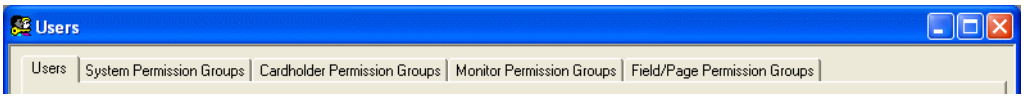
- Configure the group settings. For more information, refer to Grouping Form on page 643.
- Configure the features that are unique to the ILS locks. For more information, refer to ILS Form on page 677.
- If you want to assign priority one events to the ILS wireless locks, configure these as required. For more information, refer to ILS Priority One Events Form on page 681.

5. After adding access panels in the wizard, configure the remaining panel settings on the appropriate access panel form (for example, the LNL-3300 form).

Note: You can configure the panel, reader and lock devices individually or select the **Multiple Selection** check box to configure two or more devices.

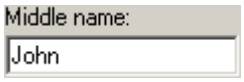
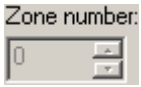
Data Entry Forms

All software setup and configuration is done through specialized windows called data entry forms. Each data entry form allows you to define the characteristics of a particular feature of the system. One or more data entry forms are logically grouped together into a folder. When you select a toolbar button or menu option, you open the associated folder. You can then display a particular form in the folder by clicking on the desired tab at the top of the form. An example is shown below:



The Users folder contains the Users, System Permission Groups, Cardholder Permission Groups, Monitor Permission Groups, and Field/Page Permission Groups data entry forms.

Form element	Example	Description
Push button	Add	A push button is a raised rectangular box. Typically, it contains a graphical image or text to indicate its purpose. Clicking on a push button performs an action.
Display	Engineer (Level 1) Engineer (Level 2) Visitor	Display fields cannot be changed directly. They are intended to provide a picture of current settings or currently defined options. On some forms, you first select an item in a display field, then enter or choose the settings for that item elsewhere on the form.
Drop-down list	Building: George Eastman Building	Drop-down list fields contain a rectangular box and a down arrow button. Clicking on the down arrow button displays a list of possible values for this field. Clicking on one of the choices inserts that value into the rectangular box. Drop-down lists are useful when there are a limited number of possible values for an item. They save data entry time, and ensure that every occurrence of a particular value is written exactly the same way.

Form element	Example	Description
Text/numeric		Text fields enable you to type whatever you want, up to the maximum number of characters allowable for that field. Text fields are used to enter information when there is a virtually unlimited number of possibilities, for things like names, addresses, and descriptions.
Spin buttons		A spin button field contains a rectangular box and a pair of buttons (down and up arrows). Clicking on the up arrow button increases the value in the rectangular box by one step. Clicking on the down arrow button lowers the value in the rectangular box by one step. Clicking and holding either button rapidly moves in that direction through the list of choices. Spin button fields are used when there are a limited number of possible values for an item, but this number can be many more than what a drop-down list typically contains. Spin button fields are typically used for numerical values.
Check box		Check box fields contain a small square box beside the name of the field. When you click on the field name, an “X” is inserted in the box to indicate that this choice is selected. Clicking on the name again removes the “X” from the box and deselects the field. When there are multiple check boxes on a form, you can select as many of them as is appropriate.
Radio button		In contrast to check boxes, radio buttons are mutually exclusive. In other words, you can only select one of them. Selecting a choice automatically deselects any previous selected choice.

Administration

CHAPTER 3

Cardholders Folder

The Cardholders folder contains forms with which you can:

- Add, modify and delete cardholder and visitor records.
- Assign cardholders or groups of cardholders to different segments.
- Create badge records for cardholders and visitors.
- Assign access levels to active badges for cardholders and visitors.
- Assign one or more Precision Access groups to a badge (if Precision Access is used on your system).
- Search for and display cardholders and visitors biometrics records.
- Search for cardholders and visitors visit records.
- Assign and track assets to cardholders and visitors.
- Link directory accounts to cardholders and visitors.
- Assign a cardholder as a tour guard.
- Assign security clearance levels to tour guards.
- Create and print reports containing cardholder information.

The folder contains up to eleven forms: the Cardholder/Visitor form, the Badge form, the Segments form (if segmentation is enabled), the Access Levels form, the Precision Access form (if in use), the Biometrics form, the Visits form, the Assets form, the Directory Accounts form, the ILS Authorization form, the Guard Tours form and the Reports form.

The Cardholders folder is displayed by selecting ***Cardholders*** from the ***Administration*** menu, or by selecting the Cardholders toolbar button.

Toolbar Shortcut

The forms in the Cardholders folder are visually divided into four sections; the right section, the upper-left section, the middle-left section and the bottom section.

Several of the form elements in these sections are common to every form in the cardholders folder. Refer to the following table for descriptions of the common form elements.

Notes: This documentation refers to cardholder data fields that are shipped as the default by Lenel. If you have used the FormsDesigner application to customize your cardholder data, the elements on your Cardholders folders will be different.

The Segments form is only available if segmentation is enabled on your system

The availability of certain forms and fields in the Cardholders folder is subject to licensing restrictions.

Cardholders Folder Fields

Photo display
Displays the cardholder's photo as it appears on their badge.

Signature display
Displays the cardholder's signature as it appears on their badge.

Last access
If ***Show Last Granted Location*** is selected in the ***Cardholder*** menu, displays information about the most recent valid access by this cardholder, including the triggered event, date, time and reader name. If ***Show Last Attempted Location*** is selected in the ***Cardholder*** menu, displays information about the most recent access attempt (whether access was granted or not) by this cardholder, including the triggered event, date, time and reader name.

Badge ID
Displays the numeric identifier assigned to the cardholder's active badge.

Issue code
Displays the issue code assigned to the cardholder's active badge.

Prints
Displays the number of times the active badge has been printed.

Activate
Displays the date when the badge becomes valid.

Deactivate
Displays the date when the badge becomes invalid.

Last name
Indicates the cardholder's last name.

First name
Indicated the cardholder's first name.

Middle name
Indicates the cardholder's middle name.

Cardholder ID
Indicates the cardholder's ID number. This field is not displayed on the Visitor form.

Badge type

Indicates the cardholder's badge type. Badge types are configured in the Badge Types folder. For more information, refer to Chapter 12: Badge Types Folder on page 307.

Search

Displayed in view mode on every form in the Cardholders folder. This button is used to search for existing cardholder records.

Add

Enabled in view mode on the Cardholder/Visitor and Badge form and is used to add a record. This button is displayed but not enabled on the Segments form, the Access Levels form, the Precision Access form, the Biometrics form, the Visits form, the Guard Tours form and the Reports form because these records are not added in the Cardholders folder.

Modify

Displayed in view mode on every form in the Cardholders folder. This button will be displayed but will not be enabled on the Directory Accounts form and the Reports form, because directory account and report records cannot be modified.

Delete

Enabled in view mode on the Cardholder/Visitor and Badge form and is used to delete a record. This button is displayed but not enabled on the Segments form, the Access Levels form, the Precision Access form, the Biometrics form, the Guard Tours form and the Reports form because these records are not deleted in the Cardholders folder.

Print

Displayed in view mode on every form in the Cardholders folder. When selected, displays the Badge Printing window from where you can print the active badge for the current record, or the active badges for all records found in a search. You can also log and print errors encountered during the print operation.

When you select this button on the Reports form, the Print Report Options window is displayed. For more information, refer to Chapter 9: Print Report Options Window on page 237.

Encode

Displayed in view mode on every form in the Cardholders folder. When clicked, displays the Encode Badge window from where you can encode the badge configurations selected for the cardholder onto a smart card. For more information, refer to Chapter 11: Card Formats Folder on page 247. The availability of this button is subject to licensing restrictions.

Replication

This field only appears on Enterprise systems. The value in this field determines where the cardholder record gets propagated. On a Master server, this option is grayed out, and "All Regions" is selected. This is because when cardholder records are added at a Master server, they must be propagated to ALL Regional servers. On a Regional server:

- If "All Regions" is selected, the cardholder record is sent to the Master server when replication occurs, and the record is then sent to ALL Regional servers when they replicate.
- If "Local Regions Only" is selected, the cardholder record is stored on the local Regional server where it was added. The record is also sent to the Master server.

First

Displayed in search mode on every form in the Cardholders folder. When selected, moves to the first record that matches your search criteria.

Rewind

Displayed in search mode on every form in the Cardholders folder. When selected, by default moves 10 matching records back. You can change the number of records moved back by modifying the value in the **Number of records to scroll for fast forward and rewind** field on the View Options window. The View Options window is displayed by selecting ***View Options*** from the ***Cardholder*** menu.

Previous

Displayed in search mode on every form in the Cardholders folder. When selected, moves to the previous record that matches your search criteria.

Next

Displayed in search mode on every form in the Cardholders folder. When selected, moves to the next record that matches your search criteria.

Fast Forward

Displayed in search mode on every form in the Cardholders folder. When selected, by default moves 10 matching records forward. You can change the number of records moved forward by modifying the value in the **Number of records to scroll for fast forward and rewind** field on the View Options window. The View Options window is displayed by selecting ***View Options*** from the ***Cardholder*** menu.

Last

Displayed in search mode on every form in the Cardholders folder. When selected, moves to the last record that matches your search criteria.

OK

Displayed in search or modify mode on every form in the Cardholders folder. When selected, saves the changes made to the current record, or begins the requested search.

Cancel

Displayed in search or modify mode on every form in the Cardholders folder. When selected, cancels the pending requested action.

Clear

Displayed in search or modify mode on every form in the Cardholders folder. When selected, clears all current record information that can be cleared from the current form.

Clear All

Displayed in search or modify mode on every form in the Cardholders folder. When selected, clears all current record information that can be cleared from all forms in the folder.

Capture

Displayed in add or modify mode on the Cardholder/Visitor form, the Segments form, the Badge form, the Access Levels form, the Precision Access form and the Biometrics form. Displayed in modify mode on the Visits form. When selected, opens Multimedia Capture. The availability of Multimedia Capture is subject to licensing restrictions.

Last Search

Displayed in search mode on every form in the Cardholders folder. When selected, retrieves the same group of records that was found by the most recent search operation.

Record count

Displayed in view mode on every form in the Cardholders folder and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.

Person type

In search mode, select the type of record you want to search. Choices are:

- All - when selected, your search will locate both Cardholder and Visitor records
- Cardholders - when selected, your search will only locate cardholder records
- Visitors - when selected, your search will only locate visitor records

Cardholders Folder Procedures

The following procedures pertain to every form in the Cardholders folder unless otherwise noted.

Cardholder Search Capabilities

Before you begin searching cardholders you must have cardholder search permissions enabled. For more information, refer to Cardholder Permission Groups Form on page 364.

In search mode, you can search on any combination of fields in the Visits folder, including the Status search, Visit and Details forms. On the E-mail and Reports forms, you can only search for the host name or visitor name.

Comparison Operators

Comparison operators are symbols that represent specific actions. You can refine your search by prefixing search fields with a comparison operator. Refer to the following table to identify the comparison operators you can use with different fields.

Comparison operator	Description	Text field	Numeric field	Drop-down list
=	Equal to	Yes	Yes	Yes
!= or <>	Not equal to	Yes	Yes	Yes
>	Greater than	Yes	Yes	NA
<	Less than	Yes	Yes	NA

Comparison operator	Description	Text field	Numeric field	Drop-down list
>=	Greater than or equal to	Yes	Yes	NA
<=	Less than or equal to	Yes	Yes	NA
%	Contains	Yes	NA	NA

Notes: "Equal to" is the default comparison operator for numeric and drop-down list fields.

If you type an equal to sign "=" in a field and nothing else, OnGuard will search for records that have an empty value for that field. For example, typing an "=" in the Department field will find every record that does not have an assigned department.

Search Fields Using "Begins With"

For text and drop-down list fields you can search records whose values begin with specific characters by entering those characters in the field. For example, when searching by last name, a filter of "L" will find "Lake", "Lewis", etc. A filter of "Lake" will find "Lake", "Lakeland", etc.

Note: The default comparison operator for text fields is "begins with".

Search Multiple Fields

When you search multiple fields, the search criteria for each field is combined. For example, typing "A" in **Last name** field and "B" in **First name** field will find all people whose last name begins with "A" and whose first name beings with "B".

One exception is searching access levels, which uses an "or" comparison for multiple selections. For example, selecting both "Access Level A" and "Access Level B" will find all cardholders with either "Access Level A" or "Access Level B" assigned.

Note: If you want to search for a range of Badge IDs, take advantage of the two Badge ID fields on the Badge form. One field is lo/cated in the middle-left section of the form and the other field is located in the right section of the form. Note, the form must be in modify mode to see both fields. Type ">= 100" in one field and "<= 200" in the other to find all badges with IDs between 100 and 200 (inclusive).

Search for a Cardholder Record

1. Select ***Cardholders*** from the ***Administration*** menu. In Alarm Monitoring, select ***Badge Info*** from the ***View*** menu.
2. The Cardholders folder opens. Click [Search].
3. If you are searching for a cardholder or visitor, select the type of person you are searching for in the **Person type** drop-down list (in the lower right). This field may not display due to licensing restrictions.
4. Specify your search criteria by typing full or partial entries in any enabled field on any of the tabs.
5. Click [OK].
6. OnGuard retrieves and displays the first matching record. Use the navigational buttons (in the lower right) to look at additional matching records.

First record/Last Record - Displays the first/last matching record.

Rewind/Fast Forward - Moves backward/forward ten matching records. To modify the number of records moved, refer to the View Options window, which is accessed from the ***Cardholder*** menu.

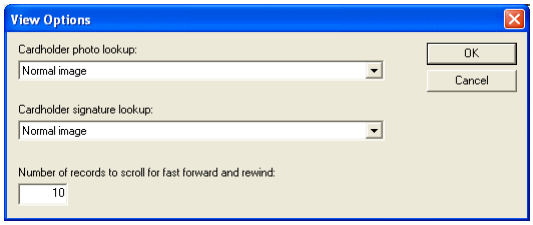
Previous record/Next record - Displays the previous/next matching record.

Retrieve the Most Recent Search Results

1. Display the Cardholders folder or Visits folder by completing one of the following:
   - To display the Cardholders folder in Alarm Monitoring, select ***Badge Info*** from the ***View*** menu. For all other applications, select ***Cardholders*** from the ***Administration*** menu.
   - To display the Visits folder in Alarm Monitoring, select ***Visits*** from the ***View*** menu. For all other applications, select ***Visits*** from the ***Administration*** menu.
2. Click [Search].
3. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
4. You can optionally modify your search criteria.
5. Click [OK].
6. OnGuard retrieves and displays the first matching record. Use the navigational buttons to look at additional matching records.

Change the Cardholders Folder View Options

1. Select ***View Options*** from the ***Cardholder*** menu. The View Options window opens.



2. From the **Cardholder photo lookup** drop-down list, select the image type you want displayed in **Photo** display (located in the right section of the Cardholders folder forms).

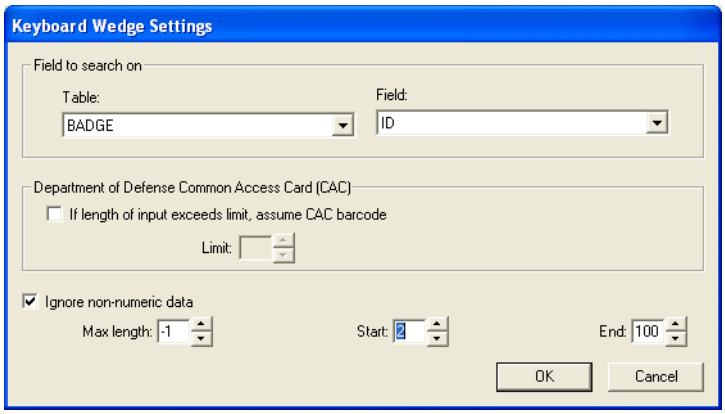
   Choices include:
   - **None** - no image will be displayed
   - **Normal image** - a photo image will be displayed as it was originally captured
   - **Normal image with chromakey** - a photo image will be displayed, but without its background
   - **Thumbnail** - This option is only displayed if the **Create/save photo thumbnails** check box in Administration > Cardholder Options > General Cardholder Options is selected. A smaller thumbnail version of the photo is displayed.
3. From the **Cardholder signature lookup** drop-down list, select the type of signature you want displayed in **Signature** display (located in the right section of the Cardholders folder forms).

   Choices include:

- **None** - no signature will be displayed
- **Normal image** - a signature will be displayed

4. In the **Number of records to scroll for fast forward and rewind** field, type in the number of records you want to move backwards and forwards when you select the and push buttons.
5. Click [OK].

Keyboard Wedge Settings Window



A wedge scanner, also sometimes referred to as a wedge reader, is a device that is attached to a keyboard and used to scan badge IDs as direct keyboard input. Wedge scanners can be used with OnGuard to:

- Add a badge. In this scenario, each card entry station has a wedge scanner. The operator clicks [Add] and swipes the badge with the wedge scanner to read the badge ID. This is equivalent to typing in the badge ID at the keyboard. When a wedge scanner is used in this man7ner, no configuration of the settings on the Keyboard Wedge Settings window is needed.
- Search for a badge. The normal way to search for a badge in OnGuard is to click [Search] and then specify what to search for, such as badge ID or social security number. When a wedge scanner is used, the [Search] button does not need to be clicked; instead, the system specifically searches on one predefined criteria. When a wedge scanner is used in this manner, the settings on the Keyboard Wedge Settings window must be properly configured.

When to Use the Keyboard Wedge Settings Window

The Keyboard Wedge Settings window only needs to be configured on systems that will be using a wedge scanner to search for badges. This may include:

- MobileVerify stations. MobileVerify stations typically use a wedge scanner because using a keyboard on a mobile computer is awkward. The wedge scanner provides a quick way to search for a cardholder and instantly grant or deny access based on the system's recommendation.
- Enterprise installations. Some Enterprise installations may choose to use a wedge scanner as a way of preventing duplicate badges. Since the card is swiped instead of typing a number in, the possibility of entering a wrong badge ID is eliminated.

The settings on the Keyboard Wedge Settings window determine the format of the data that is sent between a wedge scanner and the OnGuard system, and are specified on a per workstation basis.

Administrative rights to the workstation are required to change these settings because any changes must be written to the **ACS.INI** file.

Displaying the Keyboard Wedge Settings Window

The Keyboard Wedge Settings window is displayed by selecting ***Keyboard Wedge Settings*** from the ***Cardholder*** menu. (In System Administration, ID CredentialCenter, Visitor Management, and View/Edit Only the ***Cardholder*** menu is only displayed after selecting ***Cardholders*** from the

Administration menu. In Alarm Monitoring, the ***Cardholder*** menu is displayed after clicking the toolbar button.)

CAC Barcodes

A common access card (CAC) is a military-issued ID card that is issued to active duty personnel, selected reservists, Department of Defense civilian employees, eligible contractors, and some foreign nationals. Retirees, family members, and inactive reservists are not currently issued a CAC card.

Configuring OnGuard to Read CAC Barcodes

To set the OnGuard system up to read CAC cards, the **If length of input exceeds limit, assume CAC barcode** check box on the Keyboard Wedge Settings window must be selected. A limit also needs to be specified. If only CAC cards will be read, then the **Limit** can be set to 0. However, most systems will also need to have the ability to read other cards in addition to CACs, so the limit will need to be set to an appropriate value.

For example, a military base that assigns badge IDs to the people on its base may want to be able to read those badge IDs as well as CACs because visitors from other bases will only have a CAC. In this case, the limit would need to be set to an appropriate number. If the badge IDs were all nine digits long, then an appropriate limit would be ten because CAC barcodes are much longer than ten digits.

Scanning Barcodes with a Wedge Scanner

When an ID is scanned, OnGuard determines the length of the number that was scanned. If the number of digits exceeds the limit, then the number is treated as a CAC number, and the social security number is decrypted and searched up.

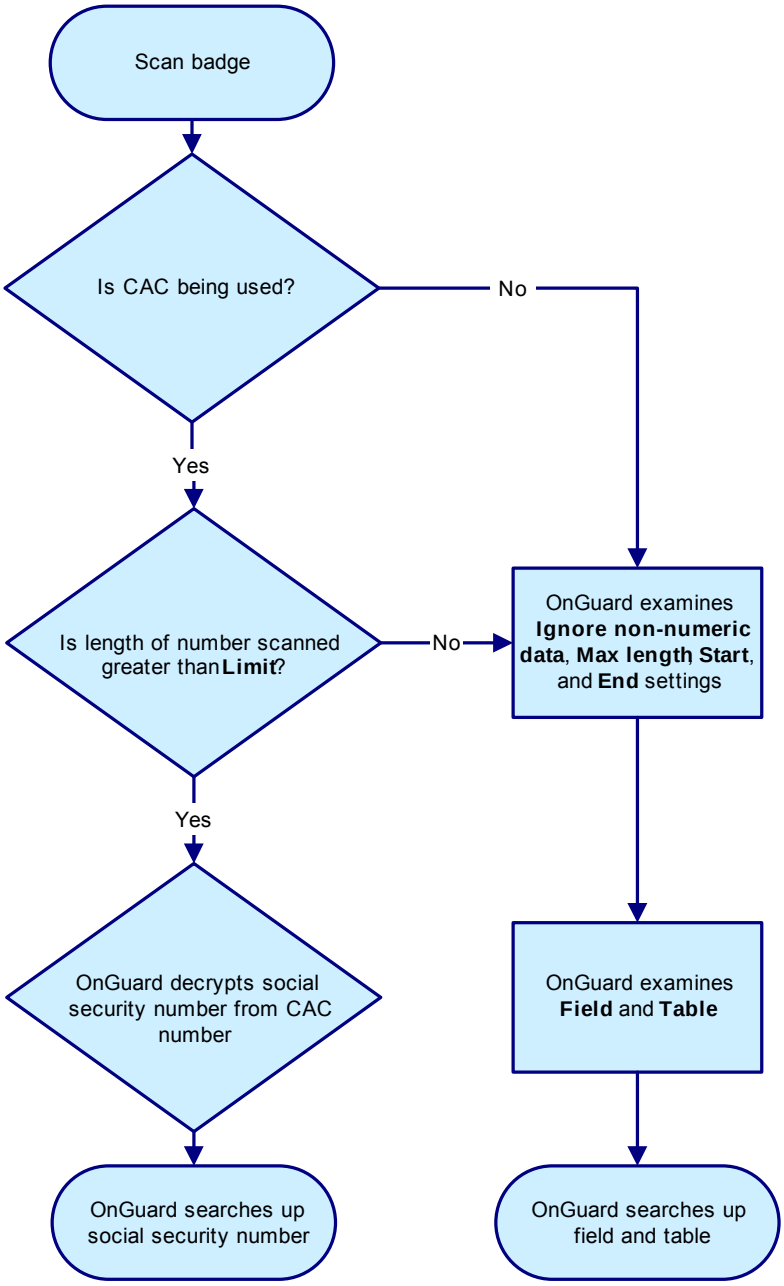
If the number of digits is less than the limit, then the maximum length, start, and end settings are applied to the string and used to extract the search criteria (typically badge ID or social security number).

After those settings are examined, the system then examines the **Table** and **Field** and searches that information up. The **Table** and **Field** specified depend on what information is encoded on the card that will be read in addition to the CAC. Common options include:

- **Badge ID**. If searching on Badge IDs, select the BADGE table and the ID field.
- **Social security number**. If searching on social security numbers, select the EMP table and the SSNO field.
- **User-defined field.** If searching on a user-defined field, select the desired table and field. For example, a company may wish to search on a table and field that is unique to their system, such as an employee number.

The following flowchart describes what happens when a barcode is scanned with a wedge scanner:

Scanning Barcodes with a Wedge Scanner



Keyboard Wedge Settings Window Fields

Table

Select the table in the OnGuard database that you wish to search on when keyboard input is detected. If searching for badge ID numbers, select the BADGE table, and if searching for social security numbers, select the EMP table. If CAC is being used and an ID is scanned that has more than the specified **Limit** of digits, then the **Table** and **Field** will be ignored.

Field

Select the field in the selected table in the OnGuard database that you wish to search on when keyboard input is detected. If searching for badge ID numbers, select ID (in the BADGE table), and if searching for social security number, select SSNO (in the EMP table). If CAC is being used and an ID is scanned that has more than the specified **Limit** of digits, then the **Table** and **Field** will be ignored.

If length of input exceeds limit, assume CAC barcode

If selected, CAC (Common Access Card) barcodes can be used. This allows military code 3of9 barcodes to be scanned and decoded into the cardholder's social security number. If you do not wish to use this feature, leave this check box deselected. If this check box is selected, you must specify an appropriate **Limit**. When this check box is selected and an ID is scanned, the number of digits will be examined.

- If the number of digits is less than or equal to the **Limit**, then the system will search on the **Table** and **Field**.
- If the number of digits is greater than the **Limit**, then the system will assume the ID was a CAC, decrypt the social security number, and search the social security number up.

Limit

The **Limit** field is only enabled when the **If length of input exceeds limit, assume CAC barcode** check box is selected.

If the **Limit** is set to zero, then only CAC can be read. Setting a limit greater than zero enables the system to recognize two different formats. When an ID is scanned, the number of digits will be examined.

- If the number of digits is less than or equal to the **Limit**, then the system will search on the **Table** and **Field** using the **Max length**, **Start**, and **End** settings.
- If the number of digits is greater than the **Limit**, then the system will assume the ID was a CAC, decrypt the social security number, and search the social security number up.

Ignore non-numeric data

If selected, non-numeric data is removed and not counted as a placeholder. This is important for scans that include dashes in the social security number. For example, if an ID is scanned that has 123-45-6789 encoded, the system will search for 123456789.

Max length

A maximum length must be provided if the wedge scanner does not automatically provide a line feed carriage return. This allows the wedge scanner to be used as long as the length of the scan is always the same (i.e., social security number).

If 0 or -1 is specified, then the whole string will be read in.

Start

The **Start** field works in combination with the **End** field. When an ID is scanned, a string of numbers are read. As long as the ID is not a CAC, that string of numbers typically contains the actual badge ID or social security number. For a CAC, that string of numbers doesn't contain the actual social security number, but OnGuard does "decrypt" the social security number from the string.

The **Start** position is important because the string of numbers may contain other numbers in addition to what is being searched for; it is the first position in the string of numbers that contains a digit of what is being searched for. The **End** position is the last digit of what is being searched for.

The **End** position should be greater than or equal to the **Start** position. Take for example the string 123456789. If 4 is the **Start** position and 7 is the **End** position, then the OnGuard system will search on 4567.

If you specify an **End** position that is less than the **Start** position, OnGuard assumes the end is 255. Therefore, for the string 123456789 with 4 as the **Start** and 3 as the **End**, OnGuard would search on 456789.

End

The **End** field works in combination with the **Start** field. As long as the ID is not a CAC, that string of numbers typically contains the actual badge ID or social security number. For a CAC, that string of numbers doesn't contain the actual social security number, but OnGuard does "decrypt" the social security number from the string.

The **Start** position is important because the string of numbers may contain other numbers in addition to what is being searched for; it is the first position in the string of numbers that contains a digit of what is being searched for. The **End** position is the last digit of what is being searched for.

The **End** position must be greater than or equal to the **Start** position. Take for example the string 123456789. If 4 is the **Start** position and 7 is the **End** position, then the OnGuard system will search on 4567.

If you specify an **End** position that is less than the **Start** position, OnGuard assumes the end is 255. Therefore, for the string 123456789 with 4 as the **Start** and 3 as the **End**, OnGuard would search on 456789.

OK

Applies the selected wedge scanner settings and closes the Keyboard Wedge Settings window.

Cancel

Closes the Keyboard Wedge Settings window without applying any changes made.

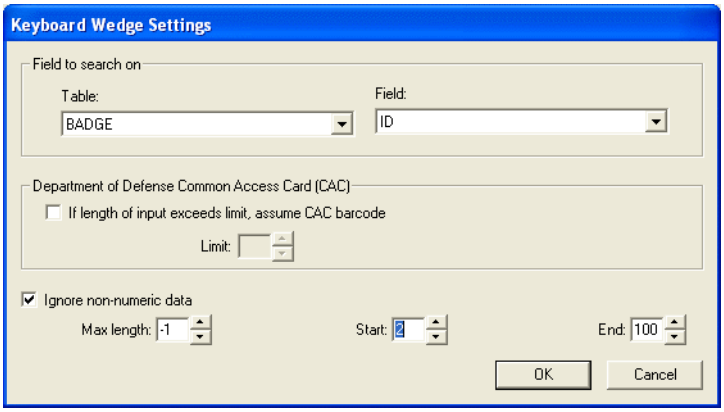
Keyboard Wedge Settings Window Procedures

The following procedures can be performed in this window.

Configure a Wedge Scanner

How the OnGuard system interprets the information it receives from a wedge scanner can be configured by doing the following:

1. In System Administration, ID CredentialCenter, Visitor Management, or View/Edit Only, select ***Cardholders*** from the ***Administration*** menu. In Alarm Monitoring, click the toolbar button.
2. Select ***Keyboard Wedge Settings*** from the ***Cardholder*** menu.
3. The Keyboard Wedge Settings window opens.



a. Specify the **Table** and **Field** you wish to search on when non-CAC input is detected. By default, the system searches on the ID field in the BADGE table. If for example you wanted to search based on social security number instead of badge ID, you would select the SSNO field in the EMP table.

b. If CAC (Common Access Card) barcodes will be used, select the **If length of input exceeds limit, assume CAC barcode** check box and specify the limit. This allows military code 3of9 barcodes to be scanned and decoded into the cardholder's social security number. If you do not wish to use this feature, leave this check box deselected.

c. Select whether to ignore non-numeric data. By default, the **Ignore non-numeric data** check box is selected. This is important for scans that include dashes in the social security number.

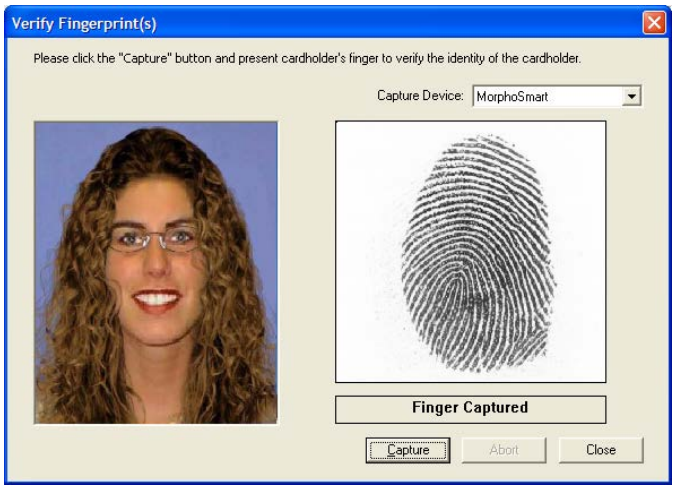
d. Specify the maximum length in the **Max length** field. A maximum length must be provided if the wedge scanner does not automatically provide a line feed carriage return. This allows the wedge scanner to be used as long as the length of the scan is always the same (i.e., social security number).

Note: If 0 or -1 is specified, then the whole string will be read in.

e. Specify the start and end. In a string of numbers that contains a search criteria (typically social security number or badge ID), start and end are the first and last position, respectively, that contain the search criteria.

f. Click [OK].

Verify Fingerprint(s) Dialog



Facial image from PIV card

If a facial image is encoded on the PIV card, it is displayed in the left pane of the dialog for verification of the cardholder's identity.

Capture Device

From the drop-down list, select the fingerprint scanning device you are using to capture the fingerprint.

Live fingerprint

The captured fingerprint is displayed in the left pane. This image is compared against the fingerprints encoded on the PIV card.

Status display

Messages and on-screen prompts are displayed in the status box below the fingerprint image.

Capture

Click this button to begin capturing the fingerprint.

Abort

Click this button to stop the capture operation.

Close

Click this button to close the dialog.

Fingerprint Verification with PIV Cards

When fingerprint data is imported from PIV cards, the Verify Fingerprint(s) dialog will be displayed allowing you to capture the cardholder's live fingerprint for comparison against the fingerprint encoded on the PIV card. If the PIV card is encoded with a facial image, it is displayed for additional verification.

IMPORTANT: Fingerprint verification is optional. To verify fingerprints, select the **Verify fingerprints on import** check box on the Cardholder Options Folder > General Cardholder Options form in System Administration. For more information, refer to Cardholder Options Folder on page 423.

Verify Fingerprint(s) Dialog Procedures

The following procedures can be performed in this dialog.

Verify Fingerprints from a PIV Card

1. When the Verify Fingerprint(s) dialog is displayed, follow the on-screen prompts provided in the status box below the fingerprint image. You will be guided through the process of capturing and verifying the fingerprints.
2. From the **Capture Device** drop-down select the device you will use to capture the fingerprints.
3. When prompted, the cardholder presents his/her finger to the capture device.
4. Click [Capture].
5. If the fingerprints match, a successful issuance is registered with OnGuard. However, if fingerprint verification fails, the card is terminated and recycled.

Note: If the PIV card contains a facial image, it is displayed with the captured fingerprint image for additional verification of the cardholder.

6. To stop the capture operation, click [Abort].

Import Fingerprints from a PIV Card

To import the fingerprints encoded on the PIV card into the database:

IMPORTANT: Ensure the **Import fingerprints from card into database** check box is selected in the Cardholder Options Folder > General Cardholder Options Form in System Administration. For more information, refer to Cardholder Options Folder on page 423.

Note: When importing data from a PIV card after adding, modifying, or searching on a badge (NOT a cardholder), cardholder-specific data that is imported (**Last name**, **First name**, **Middle name**, and **Cardholder ID**) is not overwritten even though it is displayed in the grayed-out fields. However, the cardholder photo is imported if the user confirms replacement of the existing photo.

Overwrite Facial Image Dialog

After fingerprint verification, if the cardholder already has a photo, the Overwrite Facial Image dialog is displayed allowing you to import the facial image from the PIV card and overwrite the current cardholder photo with it.

Note: Existing cardholder photos are NOT automatically overwritten. If there is an existing cardholder photo, the Overwrite Facial Image dialog is displayed with the current photo and the photo from the card allowing the user to choose which one to use.

Current Photo
Displays the cardholder's current photo.

New Photo on Card
Displays the facial image encoded on the PIV card.

Overwrite
Click this button to replace the current photo with the one on the PIV card.

Cancel
Click this button if you do not wish to overwrite the current photo.

Overwrite Facial Image Dialog Procedure

Replace Cardholder Photo with Facial Image on PIV Card

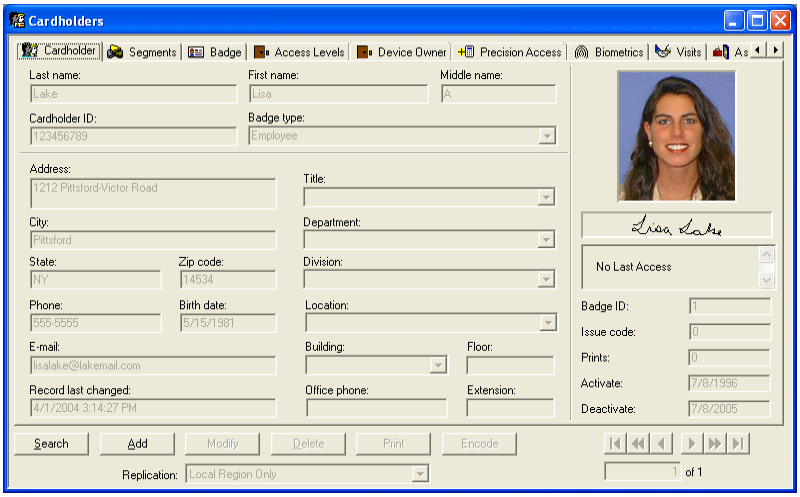
1. If the Overwrite Facial Image dialog is displayed, compare the facial image from the PIV card with the current cardholder photo.
2. Click [Overwrite] to replace the current cardholder photo with the one from the PIV card.
3. If you do not wish to replace the current cardholder photo, click [Cancel].

Cardholder Form

In the System Administration and ID CredentialCenter applications, the Cardholder form is used to:

- Define a cardholder.
- Enter or import demographic information into the cardholder record.
- Choose a badge type for the cardholder.
- Access Multimedia Capture (subject to licensing restrictions).

In the Visitor Management application, the Cardholder form is used to search for a cardholder.



Cardholder data

Displayed in view mode. When adding or modifying a cardholder record, enter the cardholder's information such as name, address and department into these fields.

Record last changed

Displayed in view mode and indicates the date on which the selected cardholder record was last modified and saved.

This date is updated only when cardholder information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

Import Cardholder/Visitor Data

Users can import demographic data stored on business cards, passports, driver's licenses, identification (ID) cards, and smart cards during cardholder/visitor add, modify, or search operations. Refer to Cardholder/Visitor Import on page 100 for a summary of the hardware used to import demographic data and the user-defined fields (UDF) that must be mapped in FormsDesigner to import data into the Cardholder form.

Note: Licenses are required to import cardholder data and are based on the number of scanning terminals used.

Prerequisites

System Administrators should complete the following steps in order to prepare OnGuard to import information:

1. Configure the reader/scanner communication settings including the workstation to which it is connected. Refer to the third column in Cardholder/Visitor Import on page 100 to determine if you have to configure the reader/scanner in OnGuard and if so, what the device type would be. For more information, refer to the Encoders/Scanners form.

Note: Some reader/scanners do not need to be configured in the OnGuard application. Simply load the drivers onto the encoding/scanning workstation.

2. Map the demographic data to the appropriate user-defined fields in Forms Designer. For more information, refer to the FormsDesigner User Guide.

3. For PIV cards:
   a. Configure the fingerprint settings in the General Cardholder Options form. For more information, refer to Cardholder Options Folder on page 423.
   b. Ensure the PIV card is inserted in the PC/SC encoder/scanner.

Cardholder/Visitor Import

Source	Hardware scanner	License required	Device Type to select in Workstations folder	Import Source to select	UDF
Business card	Corex CardScan scanner	No	NA	Corex CardScan scanner	vCard
Passport	ScanShell 1000-A Terminal	Yes	NA	ID Scan	DMV/ Passport
Driver's license	ScanShell 800-R Terminal	Yes	NA	ID Scan	DMV/ Passport
	ScanShell 1000-A Terminal	Yes	NA	ID Scan	DMV/ Passport
	ID-Check Terminal	Yes	ID-Check Terminal	ID-Check Terminal	DMV/ Passport
Identification card	ScanShell 800-R Terminal	Yes	NA	ID Scan	DMV/ Passport
	ScanShell 1000-A Terminal	Yes	NA	ID Scan	DMV/ Passport
	ID-Check Terminal	No	ID-Check Terminal	ID-Check Terminal	DMV/ Passport
GSC (iCLASS) smart card	HID iCLASS	Yes	HID (iCLASS) reader/ encoder	GSC (iCLASS) smart card	CAC GSC FASC-N
PIV card	PC/SC encoder/ scanner	No	PC/SC encoder/ scanner	PIV card	PIV FASC-N
TWIC card	PC/SC encoder/ scanner	No	PC/SC encoder/ scanner	TWIC card PIV card	PIV FASC-N

Corex Business Card Scanner

Using Corex Business Card scanners, users can import demographic data into the Cardholder form from business cards.

The Corex Business Card scanners are not configured in OnGuard as encoder/scanners. Simply load the drivers onto the encoding/scanning workstation and the Corex CardScan scanner will be an option on the Select Import Source dialog.

Only data that is mapped to the appropriate vCard -UDF or DMV-UDF field in FormsDesigner is imported into the Cardholder form.

GSC (iCLASS) Card

Using HID (iCLASS) readers/scanners, users can import demographic data into the Cardholder form from GSC (iCLASS) smart cards.

Only data that is mapped to the appropriate CAC, GSC, or FASC-N-UDF fields in FormsDesigner is imported into the Cardholder form.

Note: If badge information is stored on the smart card, you will have to assign a badge type during import.

ID Scan

Using the ID Scan scanners, users can import demographic data on driver licenses, identification cards, and passports issued by various Countries and State and Provincial Departments of Motor Vehicles.

Notes: Not all the state and provincial DMV's currently encode their driver's license and identification cards. Therefore, not all state driver licenses are supported.

Importation of cardholder and visitor data with ScanShell 800-R and ScanShell 1000-A CSS devices is now licensed. This license allows only a certain number of CSS devices, dictated by the license, to be configured through workstations and scanners.

The ScanShell 800-R is the regular scanner that scans driver's licenses and uses OCR to extract data off of them. The ScanShell 1000-A performs the same function plus passport scanning.

Only data that is mapped to the appropriate DMV-UDF fields in FormsDesigner is imported into the Cardholder form.

Data Import

Users will be prompted to select an ID, barcode, or passport during the scanning process. When ID scanning is selected users will have to select the country and the state/region of the driver license. However, when U. S. is selected (as the country), users will have an option to select auto detect (for the state). When auto detect is selected ID scan attempts to detect the state of the driver license that is being scanned.

ID-Check Terminal

Using the ID-Check Terminal scanner, users can import demographic data on driver licenses and identification cards issued by various State and Provincial Departments of Motor Vehicles. These credentials usually use any combination of a 3-track magnetic stripe, 2D barcode, and 1D barcode. Only data that is mapped to the appropriate DMV-UDF field in FormsDesigner can be imported.

Notes: Not all state and provincial DMV's are supported.

OnGuard supports ID-Check terminals (IDC-1400) version 5.4 and later.

Importation of cardholder and visitor data with the ID-Check Terminal is now licensed. This license allows only certain number of ID-Check Terminal devices, dictated by the license, to be configured.

PIV Card

Using a PC/SC encoder/scanner, users can import data into the Cardholder form from PIV cards.

Only data that is mapped to the appropriate PIV-UDF or FASC-N-UDF fields in FormsDesigner is imported into the Cardholder form.

After selecting the PIV card as the data import source, the user must enter their PIN number to authenticate the process.

Fingerprint Verification and Import

Users will be prompted to verify the cardholder's fingerprint(s) and the photo on the PIV card is presented for further verification. Fingerprints from the card may be imported as well. For more information, refer to Fingerprint Verification with PIV Cards on page 96 and Import Fingerprints from a PIV Card on page 97.

Photo Replacement

If a photo is encoded on the PIV card, the user may elect to replace the current cardholder photo with the one on the card. For more information, refer to Replace Cardholder Photo with Facial Image on PIV Card on page 98.

TWIC Card

Using a PC/SC encoder/scanner, users can import data into the Cardholder form from TWIC cards which contain both TWIC and PIV data.

Only data that is mapped to the appropriate PIV-UDF or FASC-N-UDF fields in FormsDesigner is imported into the Cardholder form.

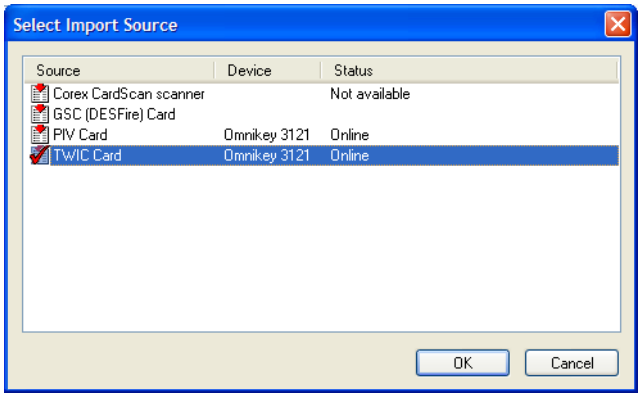
After selecting either the TWIC card or PIV card as the data import source, the user must enter their PIN number to authenticate the process.

Import Cardholder Data

1. Select ***Cardholders*** from the ***Administration*** menu for all applications except Alarm Monitoring. (In Alarm Monitoring, select ***Badge Info*** from the ***View*** menu.)
2. The Cardholders folder opens. Click [Add].

Note: The Import function is also available if the user searches for or modifies a cardholder/visitor or badge.

3. Click [Import].
4. In the Select Import Source window, select the import source available for this workstation. For more information, refer to Cardholder/Visitor Import on page 100.



Note: Import devices are configured in System Administration. In System Administration, select ***Encoders/Scanners*** from the ***Workstations*** menu.

5. Click [OK].
6. Perform the instructions that display to complete the import data process.

Cardholder Form Procedures

The following procedures can be performed on the Cardholder form.

Add a Cardholder Record

1. Select ***Cardholders*** from the ***Administration*** menu The Cardholders folder opens.
2. By default, the Cardholder form is displayed. Click [Add].
3. From the **Person type** drop-down list, select **Cardholders**.

   The **Person type** drop-down list is subject to licensing restrictions. If this field is not displayed, move on to the next step.
4. Enter the cardholder's name and any additional information in the cardholder data fields.

Note: You can switch to other tabs and modify the other forms at this time.

5. If you want to add a photograph or signature to the cardholder record, click [Capture]. Multimedia Capture opens. For more information please refer to Appendix C: Multimedia Capture on page 1339.
6. Enterprise users only: If you are adding a cardholder on a Regional server, select how the record will be replicated in the **Replication** drop-down list.
   - If you select "All Regions", the cardholder record will be sent to the Master server when replication occurs, and the record will then be sent to ALL Regional servers when they replicate.
   - If you select "Local Regions Only", the cardholder record will be stored on the local Regional server where it was added. The record will also be sent to the Master server.
7. Click [OK] to save the record.

Modify a Cardholder Record

1. Locate the cardholder record you want to change.

2. Click [Modify].
3. Make the changes you want to the record.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Cardholder Record

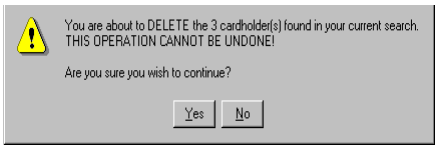
1. Locate the cardholder record you want to delete.
2. Click [Delete].
3. Click [OK].

Note: If you delete the cardholder record, all associated records (Badge, Access Levels, Precision Access, Biometrics, Assets, Directory Accounts, Guard Tours and Visits) for the cardholder are also removed from the database.

Delete a Selected Group of Cardholder Records

• WARNING! • This is a powerful feature that cannot be undone. Use caution when performing a bulk deletion of cardholders to ensure that you only delete the cardholders you want to eliminate from your database.

1. Locate the cardholder records you want to delete using the search function. The bulk delete operation will act on all cardholders that result from the current search.
2. Select ***Bulk > Delete Cardholders in Search*** from the ***Cardholder*** menu. The following message is displayed:

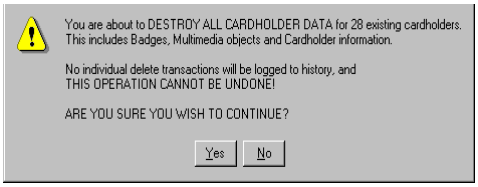


3. Click [Yes].

Destroy all Cardholder Data

• WARNING! • This feature will wipe out all cardholder and badge information from the database without any transaction logging and cannot be undone. This function is mainly intended for wiping out data after a system has been installed and tested. For example, when you are first setting up the system and have imported cardholder data but you wish to change and redo the import. This function provides a quick way to wipe out all existing cardholder data.

1. Select ***Bulk > Destroy ALL Cardholder Data*** from the ***Cardholder*** menu. The following message is displayed:



2. Click [Yes] to confirm the deletion of all cardholder data.

Visitor Form

To provide integration with Visitor Management, visitor records can be searched and viewed in the Cardholders folder. When the current record is a visitor, the first tab in the window changes from Cardholder to Visitor and will display the appropriate fields.

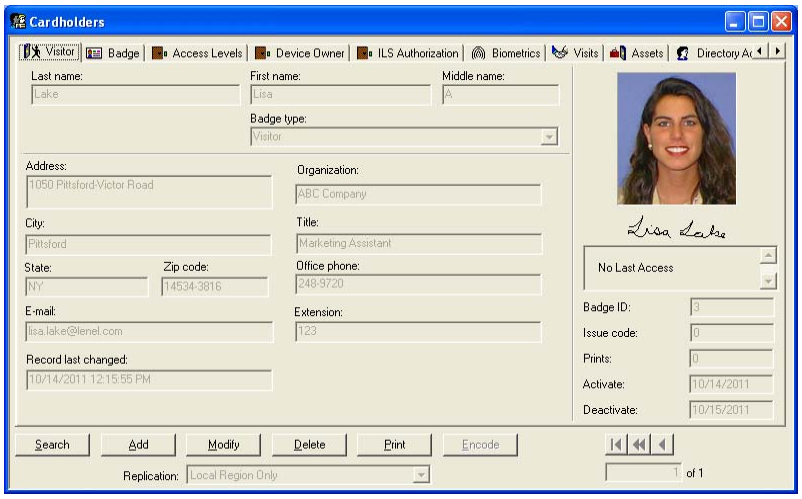
If you select the [Add] button on the Cardholder form, or the [Search] button on any of the forms in the Cardholders folder, the **Person type** drop-down list is displayed in the bottom section of the form.

The drop-down list choices are:

- All - when selected, your search will locate both Cardholder and Visitor records
- Cardholders - when selected, your search will only locate cardholder records
- Visitors - when selected, your search will only locate visitor records

Notes: With the exception of the **Allowed visitors** check box and the [Capture] button (in modify mode only) on the Visits form, visit records cannot be added, modified, or deleted from the Cardholders folder. To add, modify, or delete visits, you must purchase Visitor Management.

The availability of this form is subject to licensing restrictions.



Visitor data

Displayed in view mode. When adding or modifying a visitor record, enter the visitor's information such as name, address and organization into these fields.

Last changed

Displayed in view mode and indicates the date on which the selected visitor record was last modified and saved.

This date is updated only when visitor information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

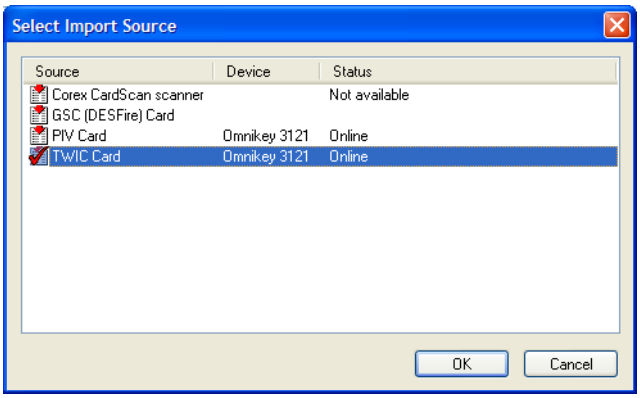
Visitor Form Procedures

The following procedures can be performed on this form.

Import Visitor Data

For more information, refer to Import Cardholder/Visitor Data on page 99.

1. In Alarm Monitoring, select ***Badge Info*** from the ***View*** menu. In all other applications, select ***Cardholders*** from the ***Administration*** menu.
2. The Cardholders folder opens. Click [Add].
3. Click [Import].
4. In the Select Import Source dialog, select the import source available for this workstation. Click [OK].



Note: Import sources are configured in System Administration under the Workstations folder > Encoders/Scanners form.

5. Follow the instructions that display. They should explain how to scan and execute the import data transaction.

Add a Visitor Record

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens. By default, the Cardholder form is displayed.
2. Click [Add].
3. From the **Person type** drop-down list, select **Visitors**.
4. Enter the visitor's name and any additional information in the visitor data fields.

Note: You can switch to other tabs and modify the other forms at this time.

5. If you want to add a photograph or signature to the visitor record, click [Capture]. Multimedia Capture opens. For more information please refer to Appendix C: Multimedia Capture on page 1339.
6. Click [OK] to save the record.

Modify a Visitor Record

1. Locate the visitor record you want to change.
2. Click [Modify].
3. Make the changes you want to the record.
4. Click [OK] button to save the changes, or the [Cancel] button to revert to the previously saved values.

Delete a Visitor Record

1. Locate the visitor record you want to delete.
2. Click [Delete].
3. Click [OK].

Note: If you delete the visitor record, all associated records (Badge, Access Levels, Precision Access, Biometrics, Assets, Directory Accounts, Guard Tours and Visits) for the visitor are also removed from the database.

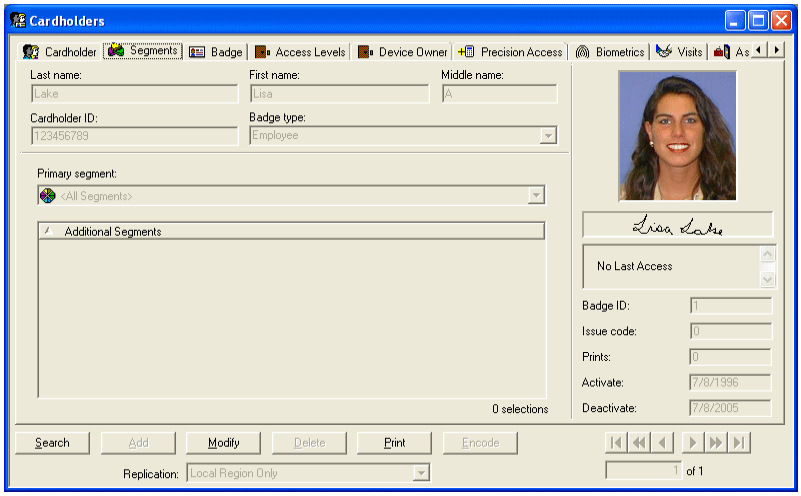
Segments Form

With segmentation enabled you may see “Restricted Entry” in the cardholder drop-down boxes. This simply means you do not have the segment permissions to view the currently configured item for cardholder.

The Segments form is used to:

- Modify a cardholder’s segment assignment.
- Change a group of cardholder’s segments.

Note: The Segments tab is only displayed if segmentation is enabled on your system.



Primary segment

In modify mode, select which primary segment you want the selected cardholder to be assigned to.

A cardholder can be assigned to a primary segment and as well as additional segments.

Additional Segments listing window

Lists all of the segments that have been configured in the system. refer to Chapter 18: Segments Folder on page 453.

Number of selections

Displays the number of segments that have been selected in the Additional Segments listing window. For example: 2 selections.

Segments Form Procedures

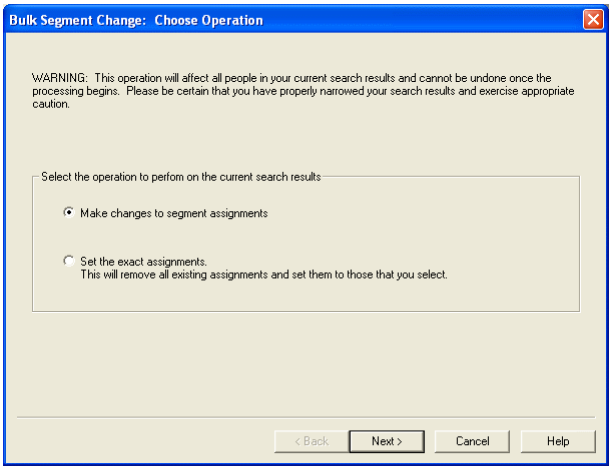
The following procedures can be performed on this form.

Modify a Cardholder's Segment Assignment

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Select the Segments tab.
3. Locate the cardholder record that you want to modify.
4. Click [Modify].
5. From the **Primary segment** drop-down list, select which primary segment you want the selected cardholder to be assigned to.
6. If you want to assign additional segments (if any exist), click on an entry in the **Additional Segments** listing window to select it. You can select multiple entries.
7. Click [OK].

Change a Group of Cardholder's Segments

1. Locate the group of cardholder records you want to change.
2. Select ***Bulk*** > ***Change Cardholder Segments*** from the ***Cardholder*** menu. The Bulk Segment Change window opens.



3. Select the **Make changes to segment assignments** radio button or select the **Set the exact assignments** radio button if you want all assignments that exist for the cardholders in your group to be replaced with the new assignments you select.
4. Click [Next].
5. Select which primary segment you want the selected groups of cardholders to be assigned to.
6. If you selected the **Set the exact assignments** radio button in step 3, and if you want to assign additional segments (if any exist), click on an entry in the Segments listing window to select it. You can select multiple entries.
7. Click [Next]. If you selected "All Segments" in step 5, proceed to step 10.

   If you selected the **Make changes to segment assignments** radio button in step 3:

   a. From the Segments listing window, select any assignments you want to add in addition to the primary segment.

b. Click [Next].

c. If there are segment assignments you want to remove from the group, click on an entry in the Segments listing window to select it. You can select multiple entries.

d. Click [Clear] to remove the assignment.

e. Click [Next].

8. If you want to perform preliminary validation and be prompted with the results before proceeding, select the **Perform preliminary validation and prompt for confirmation** radio button. Select the **Prompt only if a problem is found** check box if you do not want to a prompt for confirmation if there is no validation problem.

   If you do not want to be prompted, select the **Skip preliminary validation and perform the operation without prompting** radio button.

9. Click [Next].

10. Click [Finish].

- If you selected the **Skip preliminary validation and perform the operation without prompting** radio button in step 8 or if you selected "All Segments" in step 5, the Bulk Action Results window opens and displays a summary of your modifications. Click [OK].
- If you selected the Perform preliminary validation and prompt for confirmation radio button in step 8 and a problem was found, the Bulk Segment Validation Results window opens.

  i. Click [View Badges]. An explanation of the problem is displayed.

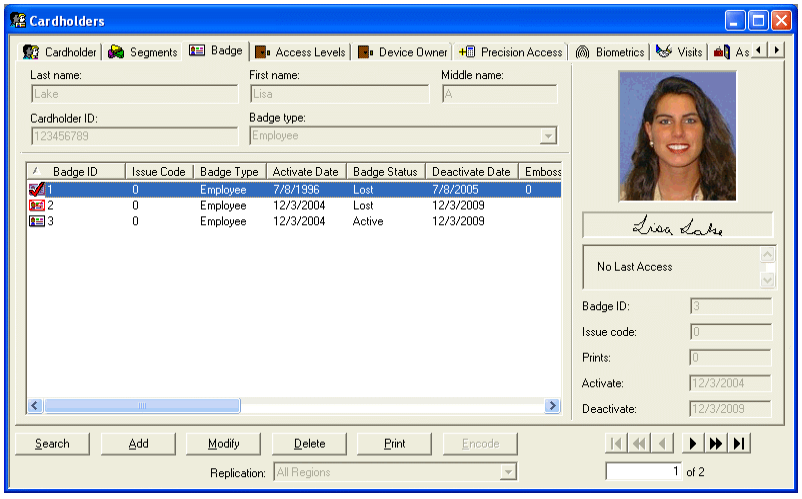
  ii. Click [OK].

  iii. Click [Continue]. The Bulk Action Results window opens and displays a summary of your modifications.

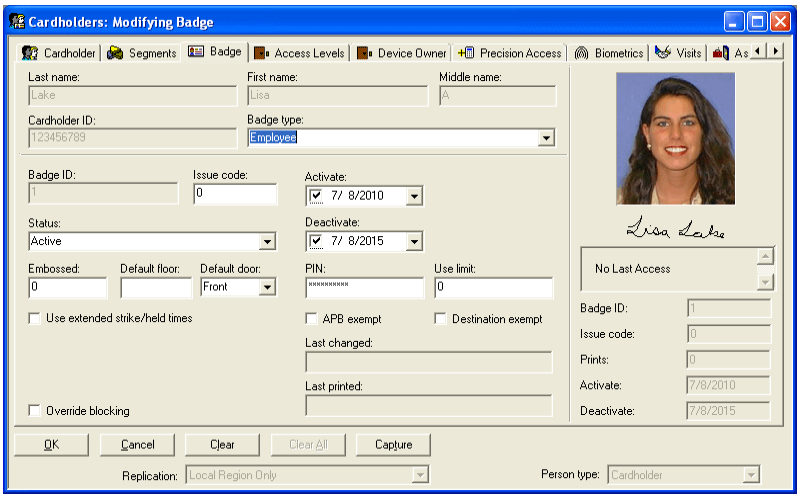
  iv. Click [OK].

Badge Form

Badge Form (View Mode)



Badge Form (Modify Mode)



Badge listing window

Displayed in view mode. Lists all badges for the selected cardholder. If you right-click on a badge in this listing window, the following options are available:

One Free Pass - If selected, allows the selected badge to violate anti-passback rules one time. This is the same as selecting ***One Free Pass*** from the ***Cardholder*** menu.

APB Move Badge - If selected, displays the Area Move Badges window from where you can move a badge to a new area. This is the same as selecting ***APB Move Badge*** from the ***Cardholder*** menu.

Encode - If selected, displays the Encode Badge window from where you can encode the badge configurations selected for this badge onto a smart card. This is the same as clicking [Encode].

Encoding History - Displays historical encoding information for the selected badge including card format, type, encoding count, and last time encoded.

Import Badge - Displays the Import Card window, in which you may select a reader to import cards from.

Import Badge ID - Displays the Encoder selection list window, in which you may select an encoder to read a badge ID from. In order for this option to be available for selection and function correctly:

- An encoder that shows <Badge ID Import> in the **Supported applications** field on the Administration > Workstations > Encoders/Scanners tab.
- The selected badge must be associated with a badge type that has “Import from card” selected in the **Generate badge ID** field on the Administration > Badge Types > Badge ID Allocation tab > ID Allocation sub-tab.
- The system should have **Maximum badge number length** on the Administration > System Options > Hardware Settings tab that is set to a value large enough to store the length of the imported Badge IDs.

Notes:

When importing badge IDs from an Omnikey or generic PC/SC encoder that supports multiple card technologies:

- If an error dialog opens stating “Incorrect card presented. *<Variable>* card was presented when iCLASS card was expected”, then you are not importing the proper card type. For more information, refer to Import Badge Information for Cards from a Mapping Table on page 327.

– If an error dialog opens stating “Unknown card with <variable> identifier presented, when iCLASS card was expected”, then the card presented is either not an iCLASS card, or it is an unknown type of iCLASS card. You can modify the ACS.INI file so that OnGuard recognizes the card as an iCLASS card. For more information, refer to Modify the CardImport Section of the ACS.INI File on page 111.

Modify the CardImport Section of the ACS.INI File

Perform the following procedure if, when importing from an iCLASS card, an error dialog opens stating “Unknown card with <variable> identifier presented, when iCLASS card was expected”:

1. Write down the value of <variable> in the error dialog.
2. Open the ACS.INI file using a text editor, such as Notepad.
3. Locate the [CardImport] section of the file.
4. Add the value of <variable> to the end of the iCLASS list.
5. Save the ACS.INI file, and then close the text editor.
6. Restart the OnGuard application.
7. Try importing the card again.

Badge ID

Displayed in add or modify mode. Indicates the numeric identifier that is assigned to this badge. The maximum Badge ID length is determined in System Administration or ID CredentialCenter in the System Options folder > Hardware Settings form (non-segmented systems) or the Segments folder > Segments form > Hardware Settings sub-tab (segmented systems).

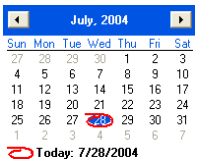
Issue code

Displayed in add or modify mode. Indicates the selected badge's issue code if your installation uses issue codes on its badges.

Activate

Displayed in add or modify mode. Indicates the date when the selected badge becomes valid.

The current date (at the time the badge record is created) is entered by default, but you can change this value by typing a numeric date into the field, or by selecting a date from the drop-down calendar.



– To select a month, click on the and navigation buttons. You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.

– Navigate to a year by clicking on the displayed year to access the year spin buttons .

– Once you have selected a month and a year, click on the day that you want the selected badge to activate on.

Deactivate

Displayed in add or modify mode. Indicates the date when the selected badge becomes invalid.

A default date is assigned based on the **Badge type**, but you can change this value by typing a numeric date into the field, or by selecting a date from the drop-down calendar.

- To select a month, click on the and navigation buttons. You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
- Navigate to a year by clicking on the displayed year to access the year spin buttons .
- Once you have selected a month and a year, click on the day that you want the selected badge to deactivate on.

Status

Displayed in add or modify mode. Indicates the badge status for the selected badge.

Status drop-down list choices are defined on the Simple Lists form of the List Builder folder.

PIN

Displayed in add or modify mode. Indicates the personal identification number for the selected badge. PIN numbers are used in conjunction with card readers that are operating in “Card and Pin,” or “Pin or Card,” mode. The maximum PIN length is determined by the **PIN type** field in the Access Panels folder.

For increased security, PIN codes are not viewable by any user. However, if the system is configured to randomly generate a new PIN code when adding a badge, the user can see the PIN code when they first add the badge (but not later).

Use limit

Displayed in add or modify mode. Imposes a restriction on the number of times a cardholder can use his/her badge at readers marked with the “Enforce Use Limit” option. A use limit value of zero (0) indicates that a badge has no uses at readers that enforce a use limit. A use limit value of 255 or that is left empty indicates that the badge has unlimited uses.

Users who have upgraded to this current build should note that the Use Limit feature has changed. Having a use limit of “0” no longer means unlimited. It now means none. A use limit of “255” now means unlimited. Also, performing a download of your system will no longer reset the uses count.

When the use limit for a badge is modified the uses left are updated to reflect the new use limit assigned. For example, if you have 10 total uses and have already used 5 (so 5 are left), and you increase the Use limit to 15, the panel will be updated so the uses left will be 10. Conversely if you have a badge with 10 total uses and have already used 5 (so 5 are left), and you decrease the Use Limit count to 8, the panel will be updated so the uses left will be 3.

Making changes to the use limit feature while your system is offline with the host may cause the badges to become out of synch with the panel.

APB exempt

Displayed in add or modify mode. When this check box is selected, any anti-passback violation for the selected badge will granted access into the anti-passback area with no violation noted in the Alarm Monitoring application.

Destination exempt

Displayed in add or modify mode. Select this check box if you want the selected badge record to be exempt from destination assurance processing.

When selected, the badge will not be included in the destination assurance processing and no alarms will be generated if the cardholder violates any of the destination assurance settings.

Via the Reports folder, you can run a Destination Assurance Exempt Cardholders report to see a list of which cardholders will be exempt from processing.

refer to Chapter 40: Destination Assurance Folder on page 825.

Use extended strike/held times

Displayed in add or modify mode. When this check box is selected, extended held open and extended strike times will be used for the selected badge. This option is supported by Lenel hardware only.

Override blocking

Select this to give the cardholder assigned to this badge the ability to unlock a door that has been blocked with a blocking card. Locks are blocked to deny entrance in unusual cases such as a police investigation. It is important to leave this field deselected unless you are certain the user of this badge template should be able to open a blocked lock. For more information, refer to Configure Blocking Cards for Integra Locks on page 1488 and Configure Special Purpose Cards for ILS Offline/Wireless Locks on page 1511.

Embossed

Displayed in add or modify mode. If applicable, enter in this field any numbers or characters that are embossed on the card. Typically this applies to Proximity cards, which are embossed by the manufacturer prior to delivery.

Default floor

Indicates which floor number is called by default when the badge is presented to a reader associated with the DEC (elevator terminal). Configure the Default floor -128 to 127. This field is only available when elevator dispatching is configured.

Ensure the **Default floor** and its **Default door** is included in the **Allowed Floors** configured for the elevator terminal. For more information, refer to Elevator Terminal Form (Terminal Configuration Sub-tab) on page 844.

Default door

Indicates which elevator door (front or rear) is opened at the **Default floor** when the badge is presented to a reader associated with the DEC (elevator terminal).

This field is only available for elevator terminals associated with a version “V2” DES or DER elevator dispatching device. For more information, refer to Elevator Dispatching Configuration Overview on page 836.

Passage Mode

Select this checkbox if you want the selected cardholder to have passage mode privileges. The passage mode privilege lets a cardholder use their card twice (within the lock's unlock duration) to place the lock in an unlock mode for an indefinite duration. The door remains unlocked until a card with the passage mode feature is used to relock the door or until a timezone with the “locked” mode becomes effective. This field is subject to licensing restrictions.

Deadbolt Override

If this checkbox is selected, the selected cardholder will have deadbolt override privileges. The deadbolt override privilege lets the cardholder access a door with a deadbolt function mortise lock even when the deadbolt is thrown. This field is subject to licensing restrictions.

Last changed

Displayed in add or modify mode. Indicates the date when the selected badge record was last saved.

Last printed

Displayed in add or modify mode. Indicates the most recent date that the selected badge was printed.

Badge Form Procedures

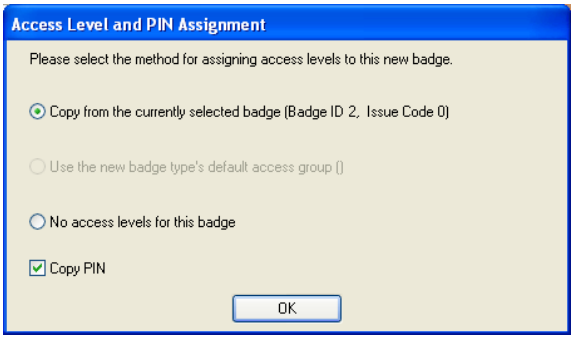
The following procedures can be performed on this form.

Add or Replace a Badge Record

1. In Alarm Monitoring, select ***Badge Info*** from the ***View*** menu. In all other applications, select ***Cardholders*** from the ***Administration*** menu.
2. Locate the existing cardholder/visitor record.
3. On the Badge tab, click [Add].
4. Select the badge type.
5. Enter the badge activation and deactivation dates.
6. Depending on how badge ID allocation is configured, you may need to manually enter a badge ID.
7. If the badge will be used for access control and access requires a card and/or personal identification number (PIN), ask the cardholder/visitor to enter a PIN.

Note: The length of PIN codes is configured in System Administration under the Access Panels folder > Options sub-tab and the Cardholder Options folder. If a PIN code is configured to be n-digits long and a cardholder enters a PIN code longer than n, the PIN code gets downloaded with the badge record, but gets truncated at n digits. For example, if a cardholder enters “123456” and the PIN type is 4-digits, then “1234” gets downloaded.

8. Enter any additional information and click [OK].
9. If this is the only active badge assigned to the cardholder/visitor, you are finished. Otherwise, continue with the next step.
10. If the cardholder/visitor record already has an active badge, the Change Badge Status dialog opens, prompting you to change the status of the “old” badge. To do this:
    a. Verify the current active (old) badge is selected.
    b. Select the new status from the **New Status** drop-down list. Choices include the default badge status values, and any badge status values that were added in the List Builder folder.
    c. Click [OK].
    d. The Access Level and Pin Assignment dialog opens, prompting you to assign an access level and PIN to the recently added (new) badge.



Note: Select the No access levels for this badge radio button to manually assign access levels or to not assign access levels at all.

e. Click [OK].

Modify a Badge Record

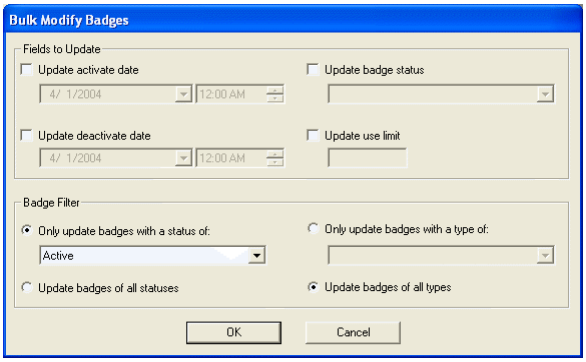
1. Locate the badge record you want to change.
2. Click [Modify].
3. Make the changes you want to the record.

Note: If the PIN type is modified on the Access Panel and/or the General Cardholder Options form, you must log off/log on before you modify a cardholder's pin number.

4. Click [OK] to save the changes, or the [Cancel] button to revert to the previously saved values.

Modify Badges for a Selected Group of Cardholders

1. Locate the group of cardholders whose records you want to modify.
2. Select ***Bulk*** > ***Modify Badges*** from the ***Cardholder*** menu. The Bulk Modify Badges window opens.



3. If you want to update the activation date, deactivation date, badge status, or use limit, do so in the Fields to Update section.

Note: The **Update use limit** field refers to the number of times a cardholder can use a badge at readers marked with the "enforce use limit" option. If you do update the use limit and leave the field empty it will be set to 255 (unlimited uses). In previous versions of OnGuard this would be set to 0, which now means 0 (or no) uses. Also note that a bulk use limit change updates a cardholder's previous use number. So, if a badge originally

was set to 5 uses, and has already used 3, and then a bulk update changed the use limit to 4, then the badge would only have 1 use left.

4. If you want to filter which badges from the selected group get modified, do so in the Badge Filter section. You can filter by badge status and/or badge type.
5. If you do not want to filter badges, select the **Update badges of all statuses** and/or **Update badges of all types** radio buttons.
6. Click [OK]. A message displays asking if you want to continue with the modification.
7. Click [Yes]. The Bulk Action Results window opens and displays a summary of your modifications.
8. Click [OK].

Encoding Prerequisites

Several steps must occur in OnGuard to properly encode a magnetic, Wiegand, or smart card. Each step occurs in a different folder in the OnGuard application.

1. In the Workstations folder > Encoding form, configure an inline or standalone encoder/scanner.

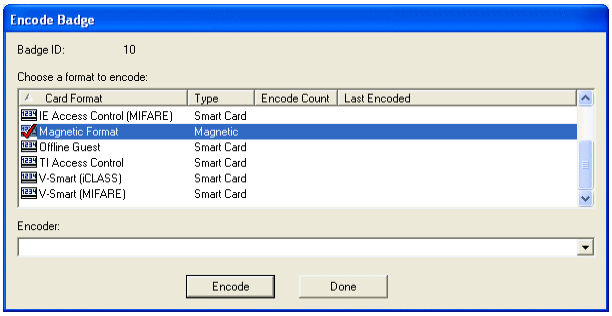
Note: You do not need to configure USB encoders/scanners (e.g. MIFARE Pegoda contactless smart card reader) in OnGuard applications. Simply install the drivers and attach the hardware to the workstation. This does not apply to the ScanShell 800-R/1000-A.

2. In the Card Formats folder, create a card format that will contain data to be encoded on a badge.
3. In the Badge Types folder > Encoding form, assign an encoding format to a badge type. In other words, assign a card format to be encoded on a badge of a specific type.
4. In the Cardholders folder, add a cardholder or visitor record to the database.
5. In Multimedia Capture, capture the cardholder/visitor's photo, signature, and/or biometric data.
6. In the Cardholders folder, encode the badge.

Encode a Badge

This procedure assumes the magnetic encoder has been set up and configured in System Administration on the Administration > Workstations > Encoders/Scanners form.

1. Display a cardholder/visitor in the Cardholders folder. You can do this by enrolling a cardholder or searching for one or several cardholders.
2. Click [Encode]. The Encode Badge window opens.



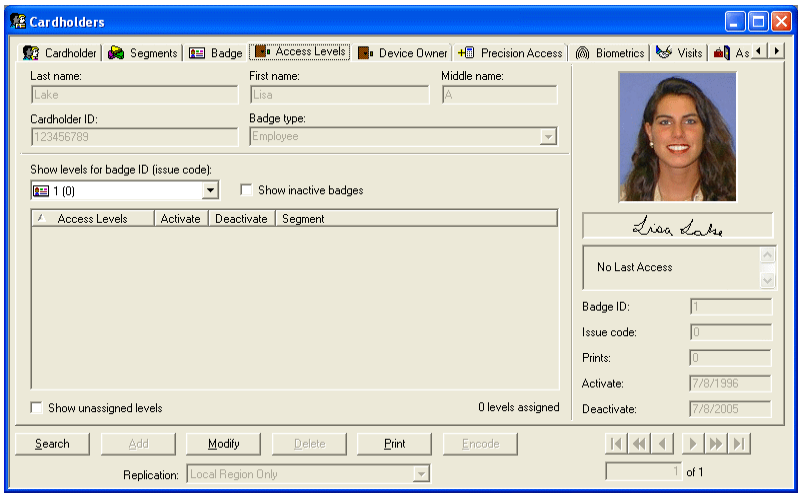
3. Select a format to encode and an **Encoder**, then click [Encode].
4. Follow the instructions that display on your monitor.

Delete a Badge Record

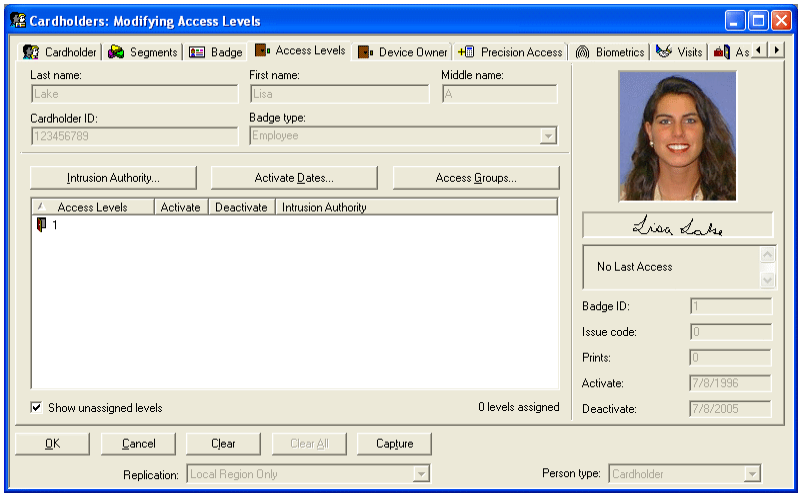
1. Locate the badge record you want to delete.
2. Click [Delete].
3. Click [OK].

Access Levels Form

Access Levels Form (View Mode)



Access Levels Form (Modify Mode)



Show levels for badge ID (issue code)

Displayed in view mode. Lists the badge ID and issue code (in parentheses) for the current active badge. If the **Show inactive badges** check box is selected, the list includes both the active and the inactive badge(s) assigned to the selected cardholder. Select a badge ID (issue code) from the list and the corresponding access levels for that badge will be displayed in the Access levels display.

Show inactive badges

Displayed in view mode. When selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected cardholder.

Access levels display

Displayed in a view and modify mode. When the **Show unassigned levels** check box is selected, lists both access levels that have been and that can be assigned to the selected cardholder/badge record. If the **Show unassigned levels** check box is not selected, only access levels that have been assigned will be listed. If they exist, also displays the access level's activation and deactivation dates.

Show unassigned levels

Displayed in view and modify mode. When selected, the Access levels display lists both access levels that have been and that can be assigned to the selected cardholder/badge record.

Number of levels assigned

Displayed in view and modify mode. Displays the number of access levels that have been assigned to the selected cardholder/badge record. For example: 6 levels assigned.

Intrusion Authority

The authority levels assigned act as access levels. Make note of this as the maximum number of access levels is usually 32.

This button is displayed in modify mode. When clicked, displays the Intrusion Authority Levels window from where you can assign intrusion authority levels. These levels will allow the cardholder the ability to issue commands via the keypad. refer to Chapter 34: Command Keypad Templates Folder on page 743.

Activate Dates

This button is displayed in modify mode. When clicked, displays the Access Level Activation Dates window from where you can select the dates when the selected access level will become valid and invalid.

Access Groups

This button is displayed in modify mode. When clicked, displays the Select Access Levels in a Group window from where you can choose the access level group that you want to select access levels from.

Access Levels Form Procedures

Note: HID Edge supports a maximum of eight (8) access levels per badge per Edge device. If you attempt to assign an access level to an HID badge that is over the 8 access levels per badge limit per device, it will not be assigned, and an error message will be displayed listing the 8 access levels already assigned to the badge.

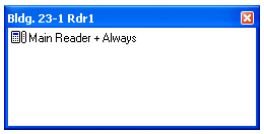
Assign Access Levels to a Badge

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Select the Access Levels tab.
3. Locate the cardholder record for which you want to assign access levels.

4. From the **Show levels for badge ID (issue code)** drop-down list, select the badge you want to assign access levels to.

   If the **Show inactive badges** check box is selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected cardholder.
5. Click [Modify].
6. Select the **Show unassigned levels** check box. The Access levels display will list both access levels that have been and that can be assigned to the selected cardholder/badge record.

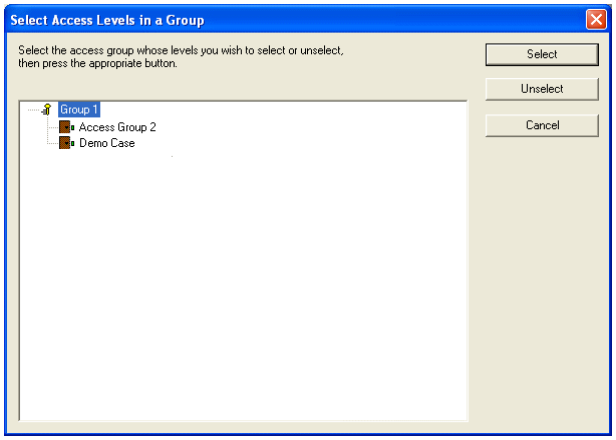
Note: To find out more about a particular access level, either double-click on an access level entry, or right-click on an access level entry and select **Level Definition**. A popup window opens, listing the reader/time zone combinations that define the access level. For example:



7. Click on an access level in the Access levels display to select it.

   Optional: If you want to assign all the access levels that belong to an access group:

   a. Click [Access Groups]. The Select Access Levels in a Group window opens.



   b. The Select Access Levels in a Group window lists all currently defined access groups. You can expand an entry to display the list of access levels that make up a group. Select an access level or an access group. If you select an access group, you select all of the access levels it contains.
   c. Click [Select].
   d. Click [Yes].
8. Repeat step 7 for each access level you want to assign.
9. Click [OK].

Assign Intrusion Authority to the Cardholder

For more information, refer to Chapter 34: Command Keypad Templates Folder on page 743.

1. On the Access Levels form, click [Modify].
2. Click [Intrusion Authority]. The Intrusion Authority Levels window opens.

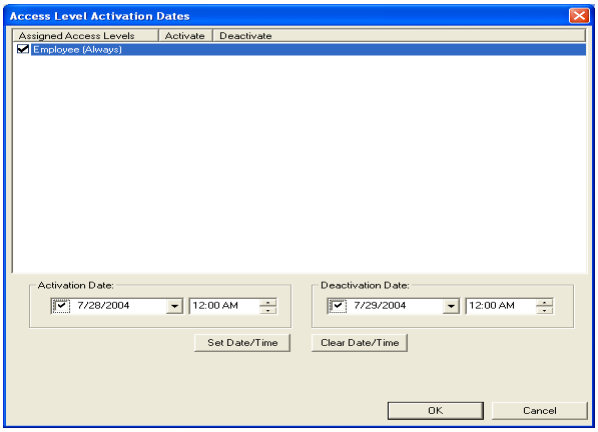
3. Select what access levels you would like to assign Level 1 and/or Level 2 authority.
4. Click [OK]. On the access levels listing window you will see an intrusion authority column that shows you what intrusion authority level(s) that access level now shares.

IMPORTANT: The authority levels assigned act as access levels but do not count toward the maximum number of access level assignment allowed per badge. When the "Advanced Permission Control" intrusion command configuration option is selected, the maximum number of access level assignments allowed per badge is reduced to 30.

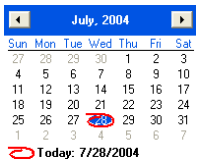
Assign Activation and Deactivation Dates to Access Levels

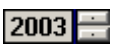
1. On the Access Levels form, click [Modify].
2. The access levels listing window displays all access levels that are currently configured for use with the selected cardholder's badge type. From the listing window, select one or more access levels.
3. Click [Activate Dates]. The Access Level Activation Dates window opens.

   The selected access levels that have been assigned to the selected cardholder/badge record will be listed in the Assigned Access Levels listing window.



4. Click on an access level entry to select it.
5. In the Activation Date section:
   a. Type a numeric date into the field, or select a date from the drop-down calendar.



   - To select a month, click on the and navigation buttons.
   - You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
   - Navigate to a year by clicking on the displayed year to access the year spin buttons  .
   - Once you have selected a month and a year, click on the day that you want the selected badge to activate on.

b. If your system is configured so that you can specify a specific activation time, enter a time in the field to the right of the date field. This time will be used in conjunction with the selected activation date.

Notes: To specify the activation time, the **Store expiration date** field on the Options sub-tab of the Access Panels form must be set to **Date only** or **Date and time**.

The activation time you enter should match the granularity setting on the Cardholder Options folder, General Cardholder Options form. Otherwise, the time you enter will be rounded down. For example if the granularity is set to 30 minutes, and you enter any time between 4:00 and 4:29 the time will automatically be rounded to 4:00. Any time entered between 4:31 and 4:59 will be rounded to 4:30.

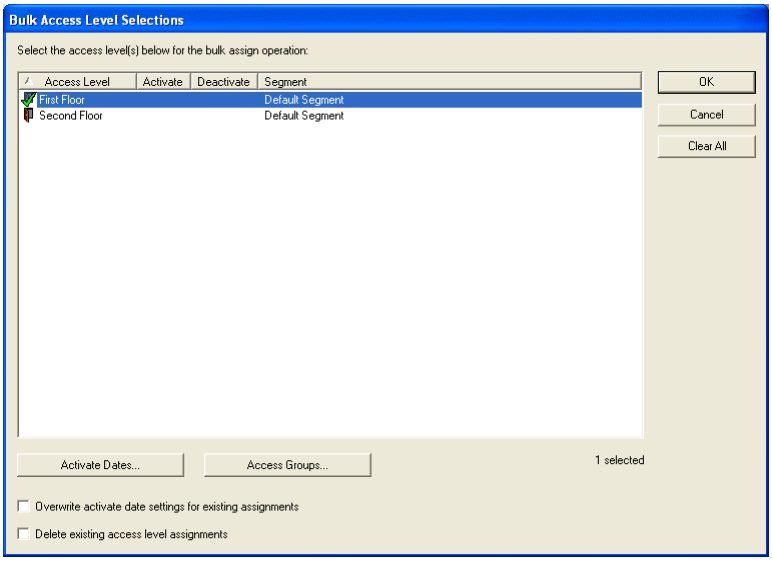
6. In the Deactivation Date section, repeat step 5, choosing the date when you want the selected badge to become invalid.
7. Click [Set Date/Time].
8. Repeat steps 4-7 for each access level entry.
9. Click [OK].

Assign Access Levels to a Selected Group of Cardholders

The linkage server is required to be running for any bulk access level update. However, since the linkage server runs independently of System Administration, it may take several minutes for the linkage server to finish processing any bulk updates even though System Administration indicates that the bulk update task is complete.

Notes: HID Edge supports a maximum of eight (8) access levels per badge per HID controller. If you attempt to assign an access level that results in more than 8 access levels going to a badge for a single HID controller, the assignment will not be allowed, and an error message will display with a list of the 8 access levels already selected for this controller.

1. Locate the group of cardholders that you want to assign access levels.
2. Select ***Bulk > Assign Access Levels*** from the ***Cardholder*** menu. The Bulk Access Levels Selections window opens.



3. To modify access levels:
   a. Select (place a checkmark beside) the access level(s) you want to assign.
   b. If you want to assign an entire access group, click [Access Groups]. Highlight the access group and click [Select].

   You can expand access groups to display associated access levels. You can also double-click access levels to display associated readers

   c. Select the **Delete existing access level assignments** check box if you want to delete the existing access level assignments and apply the new access level assignments. If you do not select this check box, the cardholders will retain their existing access levels in addition to their new access level assignments.
4. To modify activation/deactivation dates:
   a. Click [Activate Dates].The Access Level Activation Dates dialog opens.

Note: Although you can assign multiple access levels to a record, you can only assign activation/deactivation dates to one access level at a time.

   b. Select the first access level.
   c. Set the activation and deactivation dates.
   d. If there is more than one access level that you want to assign dates to, click [Set] and continue setting the activation/deactivation dates.
   e. When you are finished, click [OK].
   f. Select the **Overwrite activate date settings for existing assignments** check box to apply the new dates.
   g. Click [OK] and acknowledge any messages that display.

Remove Access Levels From a Selected Group of Cardholders

1. Locate the group of cardholders that you want to remove access levels from.
2. Select ***Bulk > Remove Access Levels*** from the ***Cardholder*** menu. The Bulk Access Levels Selections window opens.
3. Click on the access level you want to remove to select it. You can select multiple entries.

   Optional: If you want to remove all the access levels that belong to an access group:
   a. Click [Access Groups]. The Select Access Levels in a Group window opens.
   b. The Select Access Levels in a Group window lists all currently defined access groups. You can expand an entry to display the list of access levels that make up a group. Select an access level or an access group. If you select an access group, you select all of the access levels it contains.
   c. Click [Select].
   d. Click [Yes].
4. Click [OK].

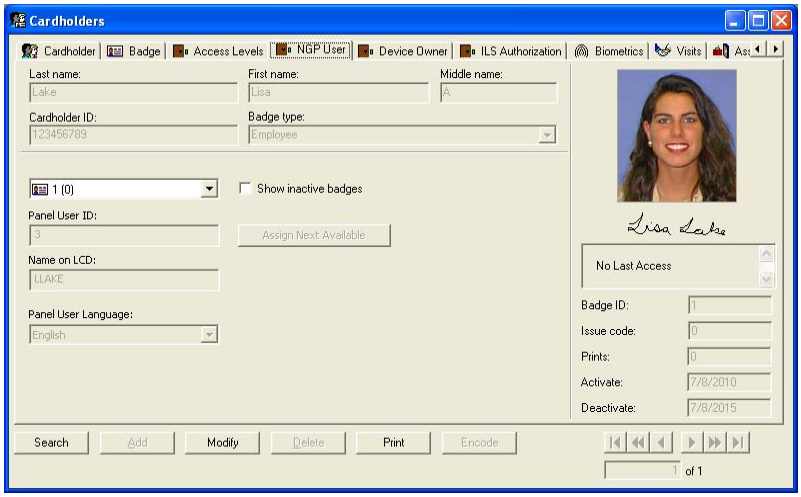
Note: All active badges will be affected by this change, even in multiple active badge environments.

Modify Access Levels Assignments

1. Locate the cardholder/badge record whose access level assignments you want to change.
2. Click [Modify].

3. Make the changes you want to the record.
   - Select the access level to assign it to a cardholder/badge record.
   - Deselect the access level to limit cardholder/badge access.
   - Click [Clear all] to deselect all the access level assignments.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

NGP User Form



Badge drop-down

Select which badge (if user has multiple badges) that will be used in the NGP system.

Show inactive badges

Select to show only inactive badges.

Panel User ID

To specify the selected cardholder as an NGP user, type a unique user ID number from 1 to 500,000 in this field, and then click [OK]. The system searches the existing user IDs to check if the number is currently in use. If the number is in use, a message is displayed with a valid range of user ID numbers. (Optionally, you can use the [Assign Next Available] button.)

Note: Before assigning a panel user ID, you must first specify a PIN code on the cardholder's Badge form.

Assign Next Available

To specify the selected cardholder as an NGP user, click this button to automatically generate the next available ID number to the cardholder. (Optionally, you can type a user ID number in the **Panel User ID** field.)

Note: Before assigning a panel user ID, you must first specify a PIN code on the cardholder's Badge form.

For more information, refer to NGP Access Panel Configuration on page 1527.

LCD name

This field is populated automatically after the cardholder is specified as an NGP user. This is the name that will display on the LCD keypad screen.

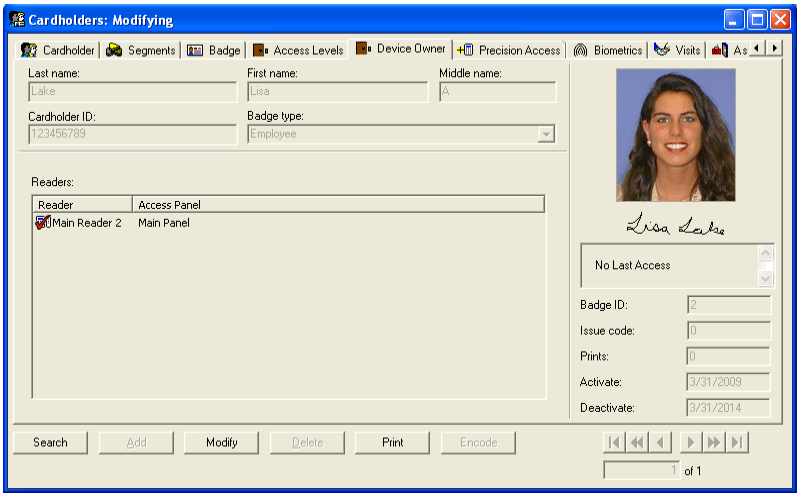
Panel User Language

Select which language the user will see when using the keypad.

NGP User Form Procedures

For more information, refer to NGP Procedures on page 1568.

Device Owner Form



Readers listing window

Lists the reader device(s) for all of the access levels belonging to the displayed cardholder. Select the reader(s) that you want the cardholder to own.

Device Owner Form Procedures

The following procedures can be performed on this form.

Assign a Cardholder to Own a Device

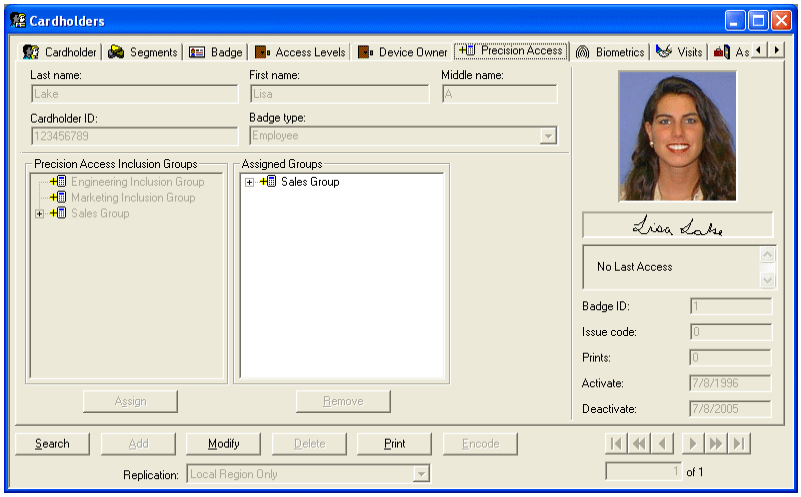
IMPORTANT: To add or modify device owners you must have device owner permissions. For more information, refer to Cardholder Permission Groups Tree on page 365.

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Select the Device Owner tab.
3. Locate the cardholder record that you want to assign to be a device owner.

4. The Readers listing window is populated with the readers that the cardholder has access to. Select the reader(s) that you wish to make the cardholder owner of.
5. Click [OK].

Precision Access Form

The Precision Access tab is only displayed if "Inclusion" is selected in the **Precision Access Mode** field on the General Cardholder Options form of the Cardholder Options folder.



Precision Access Inclusion Groups

Lists all currently defined Inclusion groups (your system will have one or the other) and the readers and timezones/elevator control levels that belong to each.

An icon precedes each inclusion group entry.

Inclusion groups are defined on the Precision Access form of the Access Levels folder.

Assigned Groups

Lists the Inclusion Groups assigned to the selected cardholder/badge record.

Assign

Assigns to the selected cardholder/badge record the access levels selected in the Precision Access Inclusion Groups field.

Remove

Removes from the current cardholder/badge record the access levels selected in the Precision Access Inclusion Groups field.

Precision Access Form Procedures

The following procedures can be performed on this form.

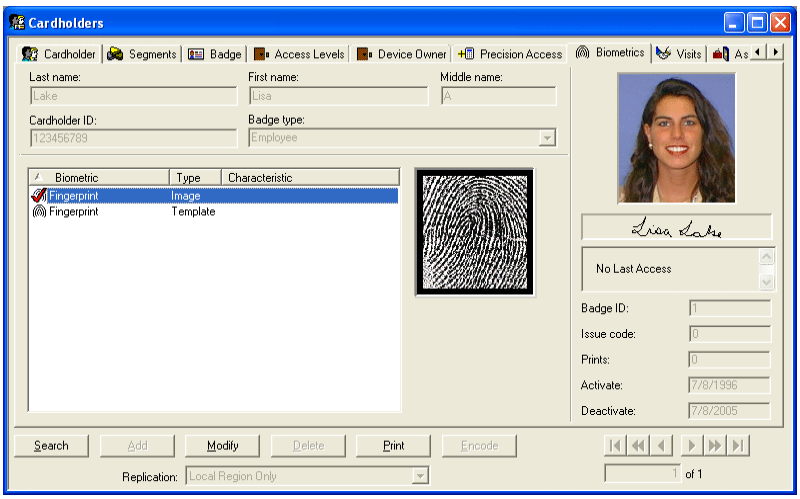
Assign Precision Access Groups to a Badge

1. Select ***Cardholders*** from the ***Administration*** menu.The Cardholders folder opens.
2. Select the Precision Access tab.
3. Locate the cardholder record that you want to assign precision access. Precision access can only be assigned to the selected cardholder's/visitor's active badge.
4. Click [Modify].
5. In the Precision Access Inclusion Groups window, select a precision access group.
   - The window contains all currently defined precision access groups. You can expand an entry to display the list of readers and timezones (if entries are Inclusion groups) that make up the group.
   - You can select only one group at a time.
   - By selecting a precision access group you select all of the reader-timezone combinations it contains. These combinations are defined on the Precision Access form of the Access Levels folder.
6. Click [Assign]. The group(s) you selected will be listed in the Assigned Groups window.
7. Repeat steps 5 and 6 for each additional group you want to assign to the badge. You can assign multiple Inclusion groups in addition to the 6 access levels that a cardholder can normally have.
8. Click [OK].

Remove Precision Access Groups From a Badge

1. Locate the record of the cardholder whose precision access assignment you want to remove.
2. In the Assigned Groups window, select the precision access group to be removed.
3. Click [Remove].
4. Repeat steps 2 and 3 for each precision access group you want to remove.
5. Click [OK].

Biometrics Form



Biometric listing window

In search mode, lists all biometric features and the type associated with each. In view mode, lists the selected cardholder's biometric information (if any exists).

There are three biometric features, Fingerprint, Hand Geometry and Iris. A biometric fingerprint's type can be template or image.

Fingerprint image

Displayed in view mode. Displays a visual representation of the cardholder's fingerprint. For more information please refer to Appendix C: Multimedia Capture on page 1339.

Search Type

Displayed in search mode. This field is used in conjunction with the listing window.

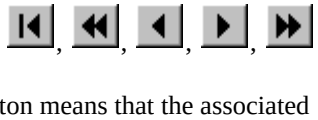
Click on a biometric feature in the listing window and select a choice from the **Search Type** drop-down list to search for a record that **Has** or **Does Not Have** a fingerprint image, a fingerprint template, iris data, or a hand geometry template associated with the cardholder.

Biometrics Form Procedures

The following procedures can be performed on this form.

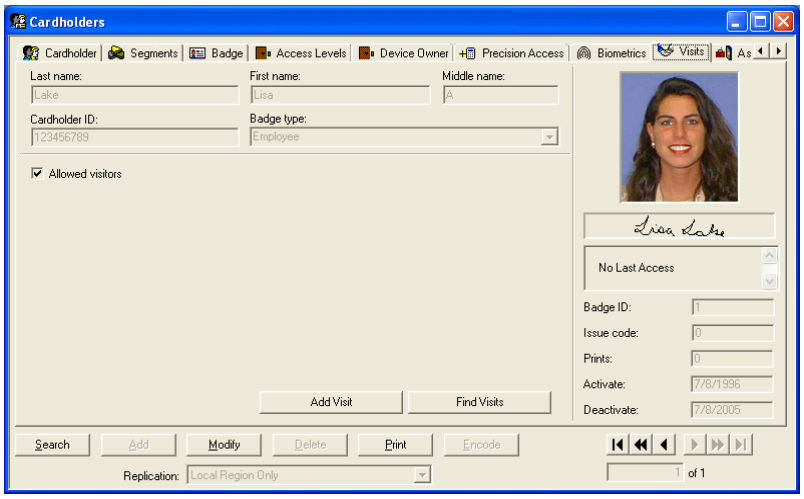
Search for a Cardholder's Biometric Record

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Select the Biometrics tab.
3. Click [Search].
4. In the Biometric listing window, click on a biometric feature to select it.
5. Choose either "Has" or "Does Not Have" from the **Search Type** drop-down list to search for a record that has or does not have specific biometric data associated with the cardholder.
6. Click [OK].

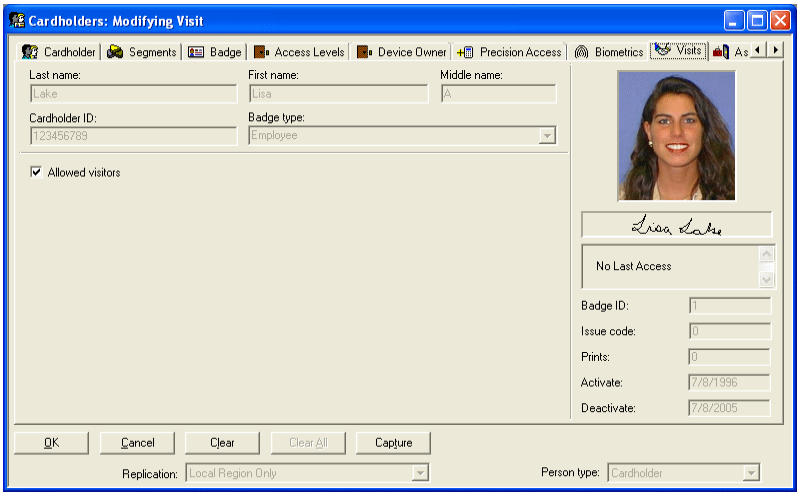
   OnGuard retrieves and displays the first matching record. Use the 
   and buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

Visits Form

Visits Form (View Mode)



Visits Form (Modify Mode)



Allowed visitors

When selected in modify mode, the selected cardholder is allowed to be assigned visitors.

When not selected, the cardholder will not be available for visit assignment in the Visitor Management application.

Add Visit

In modify mode, click this button to display the Adding Visit window. From here you can add or modify visits, display visit records for a selected date range, and search for visit records based on the scheduled time in, scheduled time out, time in, time out, or date and time last changed.

Find Visits

This button quickly looks up visit records associated with the record whose name is specified in the **Last name**, **First name** and **Middle name** fields.

Type

Displayed in modify mode. Indicates the type of visit.

Purpose

Displayed in modify mode. Indicates the purpose of the visit.

Visits Form Procedures

The following procedures can be performed on this form.

Modify a Cardholder's Permission to Have Visitors

A cardholder must have permission to have visitors visit. This permission can only be granted (or taken away) in System Administration or ID CredentialCenter, but not in Visitor Management. To change a cardholder's permission to have visitors:

1. Select ***Cardholders*** from the ***Administration*** menu.
2. Click the Cardholders tab.
3. Locate the record of the cardholder that you want to allow visitors.

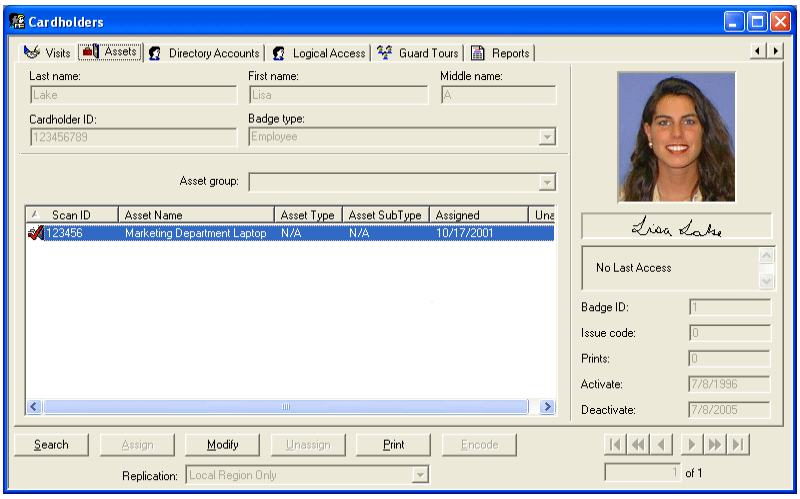
Note: Cardholders who are visitors cannot be assigned visitors.

4. Click the Visits tab.
5. Click [Modify].
6. The **Allowed visitors** check box setting controls a cardholder's permission to have visitors. Select the setting you want for the selected cardholder. The two possible settings are:
   - When the **Allow visitors** check box is selected, the cardholder will be allowed to have visitors. Only cardholders with the Allow visitors check box will be returned when searching for a cardholder and attempting to add a new visit.
   - When the **Allow visitors** check box is not selected, no visits to the cardholder can be scheduled.

Note: Changing the **Allow visitors** check box setting for a cardholder will only change the cardholder's ability to have visitors after the setting has been changed; any previously scheduled visits will be allowed to occur.

7. Click [OK].

Assets Form



Asset group
Indicates the asset group to which the cardholder or visitor belongs.

Asset listing window
Lists all assets that are currently assigned to the selected cardholder or visitor.

Assign
When selected, assigns an asset to a cardholder.

Unassign
When selected, unassigns an asset.

Assets Form Procedures

The following procedures can be performed on this form.

Assign an Asset to a Cardholder

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Select the Assets tab.
3. Locate the cardholder record for which you want to assign the asset.
4. While still on the Assets tab, locate the asset record that you want to assign.
5. Click [Assign].

Note: Authorized users can manually assign an asset to a cardholder who does not have proper asset group permissions for that asset.

Unassign an Asset

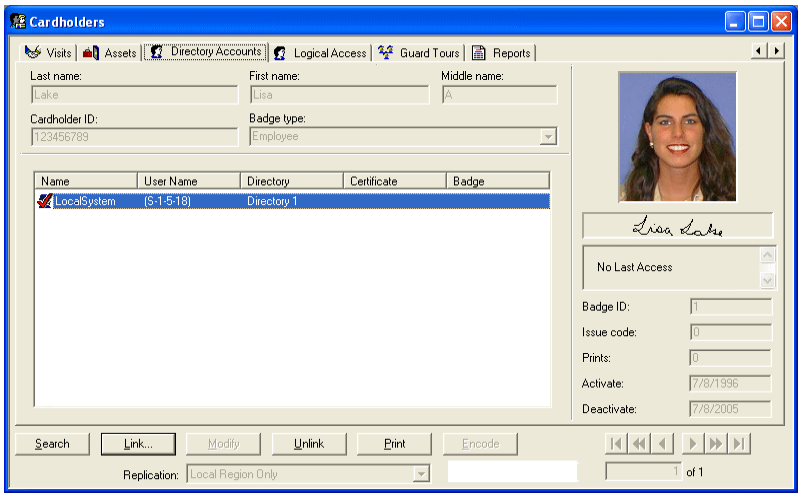
1. In the Asset listing window, click on the name of an asset to select it.
2. Click [Unassign].

Modify the Asset Group

1. Locate the cardholder record for which you want to modify.
2. Click [Modify].
3. Select an Asset Group from the drop-down list.
4. Click [OK].

Note: A record can only be modified if an asset group was assigned when the cardholder or visitor was added.

Directory Accounts Form



Directory accounts listing window
Lists the directory accounts that have been linked to the selected cardholder.

Link
When selected, displays the Select Account window from where you can link a directory account to the selected cardholder.

Unlink
When selected, unlinks the selected cardholder from the directory account that is selected in the Directory Accounts listing window.

Directory Accounts Form Procedures

The following procedures can be performed on this form.

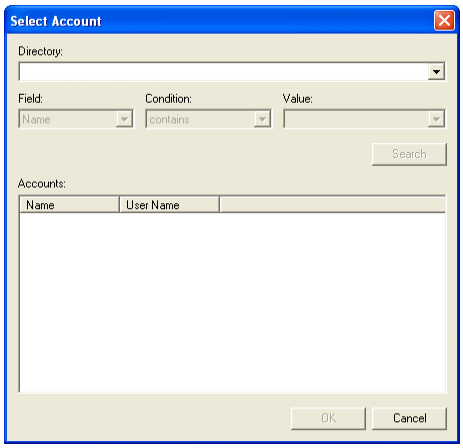
Link a Cardholder to a Directory Account

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Select the Directory Accounts tab.

3. Locate the cardholder record for which you want to link a directory account.
4. Click [Link]. The Select Account window opens. In the Select Account window:
   a. In the **Directory** drop-down list, select the directory you wish to link to.
   b. In the **Field** drop-down list select whether to search for a name or user name.
   c. In the **Condition** drop-down list, select how the value will be related to the field. For example, a search where the **Field** selected is “Name”, the **Condition** selected is “contains” and the **Value** specified is “Lake” will display all accounts where the name contains the word “Lake”, such as Lisa Lake.
   d. In the **Value** field, type or select a word you think may be in the user name or name. If you leave this field empty, all accounts for the selected directory will be displayed when the search is executed.

Note: To help you search, the **Value** field will contain different ways that the selected account may be expressed. For example, if the user account Lisa Lake is selected, the permutations listed might be “L. Lake”, “LISA”, “Lisa”, “Lisa L.”, “Lisa Lake”, “LL”, “Lake” and “Lake, Lisa.”

   e. Click [Search].
   f. The accounts associated with the selected **Directory** will be displayed in the Accounts listing window.
      - If the account you wish to link to is displayed, select it. Your window should look similar to the following:



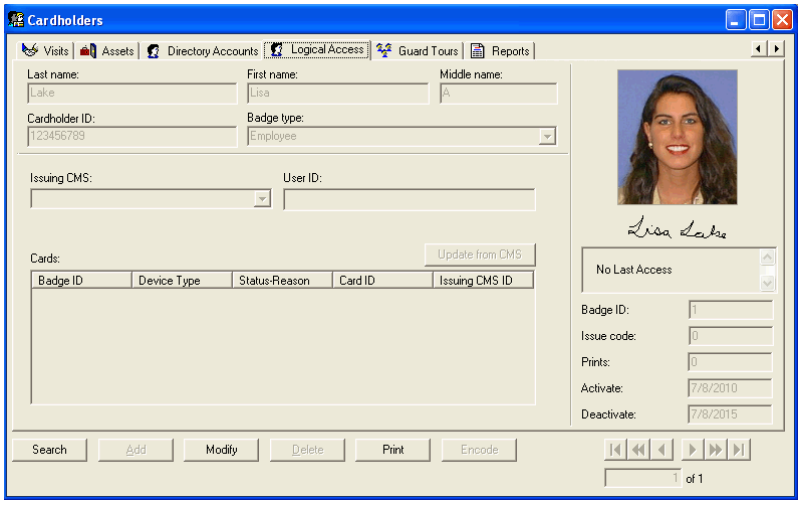
      - If the account you wish to link to is not displayed, return to step d and select another **Value** to search for.
   g. Click [OK].
   h. Repeat steps 3 and 4 for each directory account you wish to link to the selected user account.
5. Click the [OK] button on the Directory Accounts form.

Unlink a Directory Account

1. Locate the record of the cardholder you want to unlink a directory account from.
2. Click on an entry in the Directory accounts listing window to select it.
3. Click [Unlink].
4. Click [OK].

Logical Access Form

Before a badge can be issued to a user, the cardholder record for the user must have a logical user account linked to it on this form. Displayed by: ***Administration > Cardholders > Logical Access form***.



Issuing CMS

The CMS that the user exists in. It will be the CMS that is connected to when issuing a badge to the cardholder.

User ID

The cardholder's logical user account name.

Cards listing window

Lists all cards/badges that have been encoded or bound to the cardholder. Additional operations on the badge (such as resuming, suspending, terminating, or unlinking) can be performed by right-clicking on an entry in the list.

Update from CMS

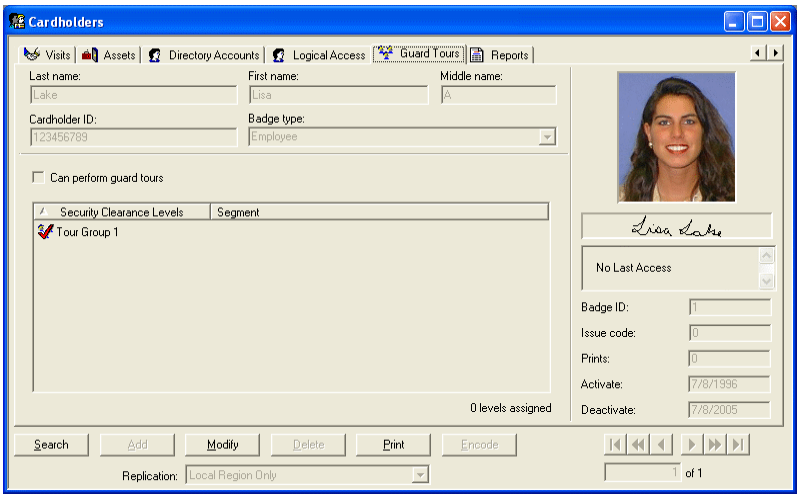
Allows badges that have been issued to the user outside of OnGuard to be displayed in the Cards listing window. Badges issued to users outside of OnGuard cannot be linked to a physical badge and thus do not support life cycle management.

Logical Access Form (Cardholders Folder) Procedures

For instructions on how to configure and use CMS, refer to Appendix I: Integrating ActivIdentity CMS with OnGuard on page 1453.. The following procedures in that section are performed using the Logical Access Form in the Cardholders folder:

- Encode/Bind a CMS Card on page 1464
- Encode/Bind a PIV Card on page 1465
- Manage Lost Badges on Systems Integrated with ActivIdentity CMS on page 1468

Guard Tours Form



Can perform guard tours

Select this check box to if you want the selected cardholder to perform guard tours.

Security Clearance Levels listing window

Lists all security clearance levels that have been configured in the system. Security clearance levels are a means of limiting the number of tour guards to choose from when a tour is launched. Particular security clearance levels will be assigned only to guards who will need access to areas where a tour will take them. When a tour is launched, only guards with the appropriate security clearance level for that tour will be listed.

Guard tours and security clearance levels are configured in the Guard Tour folder. refer to Chapter 45: Guard Tour Folder on page 891.

This field is enabled only if the **Can perform guard tours** check box is selected.

Number of levels assigned

Displays the number of security clearance levels that have been assigned to the selected cardholder. For example: 6 levels assigned.

Guard Tours Form Procedures

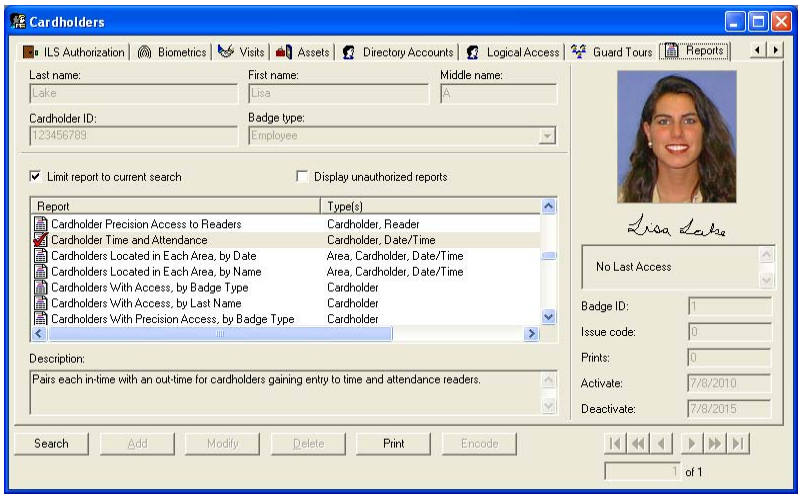
The following procedures can be performed on this form.

Assign Guard Tour Security Clearance Levels to a Cardholder

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Select the Guard Tours tab.
3. Locate the cardholder record for which you want to assign security clearance levels.
4. Click [Modify].
5. Select the **Can perform guard tours** check box.
6. In the Security Clearance Levels listing window, click on an entry to select it.
7. Click [OK].

Note: You can assign multiple security clearance levels to a cardholder.

Reports Form



Limit report to current search

When selected, only cardholders in the current search will be included in the report.

Display unauthorized reports

By default, the reports form only lists reports that users have permissions to preview. If the **Display unauthorized reports** check box is selected, reports that are disabled for a user will appear in the Report listing window. The user can identify which reports are disabled by whether the [Print] button is inactive. This allows the user to ask the system administrator for permission to an existing report, if desired.

Reports are authorized and unauthorized by using report permission groups. For more information, refer to Report Permission Groups Form on page 371.

Report listing window

Lists currently defined cardholder-related reports.

Description

A brief description of the report contents.

Reports Form Procedures

The following procedures can be performed on this form.

Run a Cardholder Report

1. Select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Select the Reports tab.

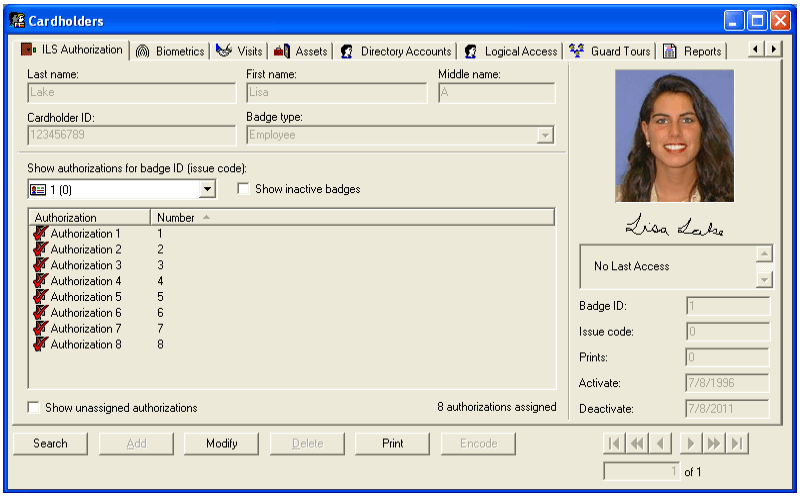
3. Locate the cardholder record(s) for which you want to run a report. (If you want to run a report on all cardholder records, skip this step.)
4. In the Reports listing window, click on the name of the report you want to run.
5. Select the **Limit report to current search** check box if you want only cardholders in the current search to be included in the report. If you do not select this check box, all cardholder who meet the criteria specified in the **Description** field will be included in the report.
6. Click [Print]. The Print Report Options window opens. refer to Chapter 9: Print Report Options Window on page 237.

Note: Any report in the Reports List Window on the Event Reports form in the Reports folder that has “Cardholder” listed in the Type(s) column is available on the Reports form in the Cardholders folder. This means that a report can be generated on the Reports form in the Cardholders folder based on a cardholder search operation.

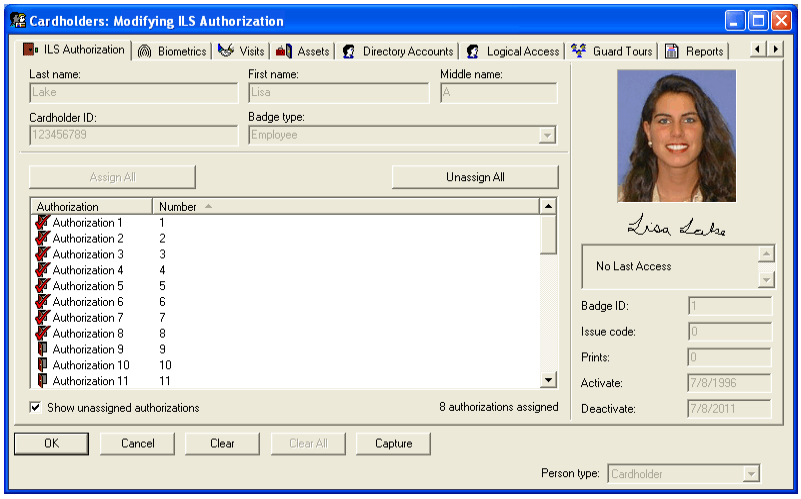
ILS Authorization Form

Note: To view these forms your system must have an ILS license.

ILS Authorization Form (View Mode)



ILS Authorization Form (Modify Mode)



Listing window

Lists the ILS authorizations that can be assigned to the cardholder.

Show authorizations for badge ID (issue code)

Displayed in view mode. Lists the badge ID and issue code (in parentheses) for the current active badge. If the **Show inactive badges** check box is selected, the list includes both the active and the inactive badge(s) assigned to the selected cardholder. Select a badge ID (issue code) from the list and the corresponding access levels for that badge will be displayed in the authorization listing window.

Show inactive badges

Displayed in view mode. When selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected cardholder.

Show unassigned levels

Displayed in view and modify mode. When selected, the authorization listing window lists both access levels that have been and that can be assigned to the selected cardholder/badge record.

Assign All

Displayed in modify mode. Click to assign all authorizations displayed in the authorization listing window.

Unassign All

Displayed in modify mode. Click to unassign all authorizations displayed in the authorization listing window.

ILS Authorization Form Procedures

To read how to configure an ILS locking system, refer to Appendix K: Lenel ILS (Integrated Locking Solutions) on page 1473.

CHAPTER 4

Badge Print Preview Window

The Badge Print Preview window is used to:

- View (on-screen) a badge to be printed from the Cardholders folder.
- Print a badge.

This window is displayed by clicking [Print] in the Cardholders folder and then clicking [Print Preview], or by selecting ***Print*** from the ***Application*** menu. The ***Application*** menu is only available in System Administration and ID CredentialCenter.

Preview window

Displays the currently selected badge layout with cardholder information.

Print All

Prints all the badges selected according to the Badge Printing window.

Print Current

Prints the badge that is currently displayed in the preview window.

Close

Click on this button to exit from the Badge Print Preview window.

Next Page

Allows you to view the next badge if multiple badges are being printed or to view the back layout of a two-sided badge.

Previous Page

Allows you to view the previous badge if multiple badges are being printed or to view the front layout of a two-sided badge.

Help

Displays online help for this topic.

Zoom

Enter a value to zoom in or zoom out on the badge in the preview window. Entering a number greater than 100% will cause the preview to zoom in on the badge, displaying less area and more detail. Entering a number less than 100% will cause the preview to zoom out on the badge, display more area and less detail

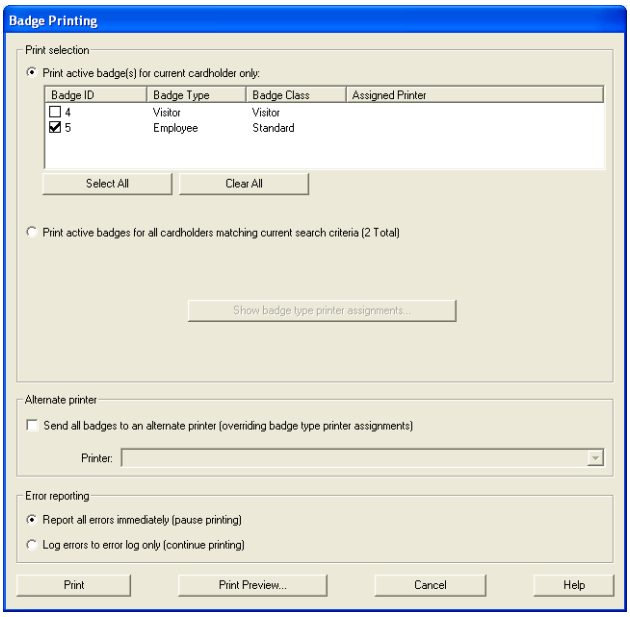
Badge information

Displays badge and cardholder information for the badge currently in the print preview window. Printer information displays also.

Page number

Displays the number of the page or badge that is currently in the preview window.

Badge Printing Form



Print active badge(s) for current cardholder only

Select this to print the active badges currently shown on the Cardholders form. By default, the active badge currently selected on the Cardholder form is selected to print. If other active badges exist for the cardholder, these will be included and may be selected to print as well.

Select All
Click to select all badges of the current cardholder.

Clear All
Click to de-select all badges of the current cardholder.

Print active badges for all cardholders
Select this option to print all active badges that match the search criteria currently in the Cardholders form.

Show badge type printer assignments
Click to show what printer is assigned to the current print selection.

Send all badges to an alternate printer
Select to open the Printer dialog box which allows you to select a printer other than the one assigned.

Printer
Select what printer should be used.

Report all errors immediately (pause printing)
Select to pause the printing when an error occurs. Selecting this causes errors to be reported immediately.

Log errors to error log only (continue printing)
Select this to continue printing when errors occur. Selecting this causes errors to be logged for further review.

Print
Click to print your current selection.

Print Preview
Click to preview what will be printed.

Cancel
Closes the Badge Printing form.

Badge Print Preview Window Procedures

The following procedures can be performed in this window.

Preview and Print a Badge

1. Select an active badge from within the Cardholders folder (Cardholders, Badge, Access Levels, Assets or Precision Access form).
   - Before printing, make sure that you are properly configured to print badges. Configurations are done using the Badge Types and Card Formats folders in System Administration or ID CredentialCenter.

- Make sure the proper printer is chosen. This is configured by selecting ***Badge Types*** from the ***Administration*** menu in System Administration or ID CredentialCenter and setting the printer assignments on the Printing/Encoding folder.

2. Do one of the following:
   - Select ***Print*** from the ***Application*** menu.
   - Click [Print] on any form within the Cardholders folder (Cardholders, Badge, Access Levels, Assets or Precision Access form).
3. The Badge Printing window displays.
   - The Print selection section determines which badges are printed or previewed out of the cardholders listed in the current search results.
     - To print/preview specific badges for the current cardholder select **Print active badge(s) for current cardholder only**. The badge selected within the Cardholder form is selected by default. If multiple active badges are included in the list, select any of these to print or preview as well. Only the active badges for the current cardholder display in the Print selection section.
     - To print all the active badges for the current cardholder select **Print active badges for all cardholders matching current search criteria**. If you click [Show badge type printer assignments] the following information displays within the Badge Printing window: Badge Type, Primary Segment and Assigned Printer.

   Notes: Badges will not print if at least one badge does not have a printer assigned to it or at least one badge has been assigned to a printer that OnGuard no longer recognizes. You must establish a network connection to a remote printer (via control panel) in order OnGuard to recognize that printer.

   To be printable, a badge must be active, have a print count of zero if you do not have permission to print duplicates or a print count less than the maximum number of prints for its badge type if you have permission to print duplicates. Also, a badge must have a front and/or back layout assigned to its badge type.

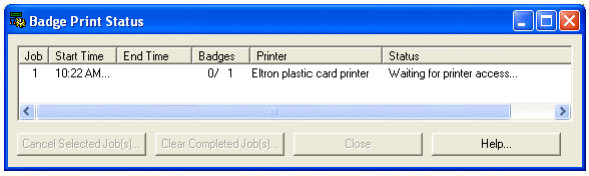
   - The Alternate printer section allows you to override badge type printer assignments and send all badges to an alternate printer. This section is only active when an alternate printer is configured and the user has permission to choose an alternate printer. For more information, refer to Modify a Print Setup on page 316. For more information, refer to Cardholder Permission Groups Form Procedures on page 366.
   - The Error Reporting section allows you to configure how printing errors are handled. All badge printing is logged to the transaction log (print previews are not logged).
     - Click the **Report all errors immediately (pause printing)** radio button if you want to be prompted to either abort printing or skip to the next badge (or badge type) when an error occurs.
     - Click the **Log errors to error log only (continue printing)** radio button if you want errors logged and badge printing to continue on to the next badge (or if the error is associated with the badge type, the printing will move onto the next badge type).
4. It is recommended that you preview your badges first before printing them. If there is no need to preview the badge(s), you may print at this time by clicking [Print]. Skip to step 9. If you wish to exit the window without printing, click [Cancel]. Otherwise continue on to the next step.
5. Click [Print Preview] to display the Badge Print Preview window.

The current badge displays along with cardholder data and printer information.

6. Use the [Next Page] and [Previous Page] buttons to view the next badge or other side of a two-sided badge.
7. You can zoom in or out on the badge by changing the percentage value in the **Zoom** box. A larger number displays the badge close-up, in more detail. A smaller number will display more of the badge, in less detail.
8. To print the badge(s), do one of the following:
   - Click [Print Current]. Doing so will print the badge that is currently in the preview window.
   - Click [Print All] to print all of the badges that have been selected.
   - To exit from the window without printing, click [Close].

Note: If a user attempts to print a badge that has already been printed the maximum number of times then an error displays and the badge does not print. As with other printing errors the user can continue on to the next badge if a batch print is being performed.

9. If you decided to print badges a status window displays to indicate the status of the print operation.



A single print job entry represents all the badges selected in the Print selection section.

CHAPTER 5

Visits Folder

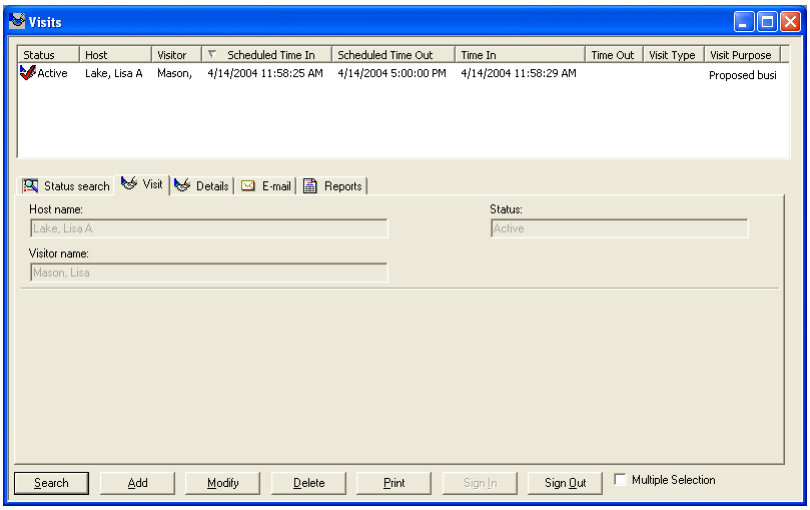
The Visits folder contains the Status search form, the Visit form, the Details form, the E-mail form and the Reports form with which you can:

- Display visit records for a selected date range
- Search for visit records based on the scheduled time in, scheduled time out, time in, time out or date and time it was last changed
- Display visit records that are scheduled in the future, scheduled and are late, active, active and overstayed and finished
- Filter and display visit records for a selected cardholder, visitor or both
- Display the cardholder or visitor record associated with a visit
- Refresh the Visits listing window
- Send e-mail notifications regarding visits
- Add or modify visits
- Delete a visit or multiple visits
- Print a disposable badge or multiple disposable badges
- Sign out and sign in a visit or multiple visits
- Generate a report for either a defined search criteria or for all visits

This folder is displayed by selecting ***Visits*** from the ***Administration*** menu or by selecting the Visits toolbar button.

Toolbar Shortcut

The forms in the Visits folder are divided into two sections: the form elements that are common to every form in the Visits folder (shown in the screen shot that follows) and the form elements that are unique to each form. For descriptions of the common form elements refer to Visits Folder Fields on page 147. For descriptions of the unique form elements refer to Status Search Form on page 162, Visit Form on page 159, Details Form on page 163, and E-mail Form on page 164, and Reports Form on page 166.



Notes: This documentation refers to visit data fields that are shipped as the default by Lenel. If you have used the FormsDesigner application to customize your visit data, the elements on your Visits folder forms will be different.

Forms and fields that pertain to segmentation are only available if segmentation is enabled on your system.

Visit Right-Click Menu

If you right-click on a visit in the listing window, a menu will be displayed. The menu contains the following options.

Menu Options

Select All

Enabled only when the **Multiple Selection** check box is selected. If selected, all visits in the listing window will be selected.

Clear All

If selected, all visits selected in the listing window will be deselected.

Add

Selecting this option does the same thing as clicking the [Add] button - it allows you to add another visit based on the currently selected visit.

Modify

Selecting this option does the same thing as clicking the [Modify] button - it allows you to change the visit that is currently selected.

Delete

Selecting this option does the same thing as clicking the [Delete] button - it allows you to delete the visit that is currently selected. The visit will be deleted without prompting for confirmation.

Sign In

This option is only available for a visit that is not active/not signed in. If the **Multiple Selection** check box is selected, multiple visits can be selected and signed in at once. Selecting this option does the same thing as clicking the [Sign In] button. If selected, the Sign In Visit(s) window is displayed. In this window, select whether to print disposable badges for the visitor that is being signed in.

Sign Out

This option is only available for a visit that is active/signed in. If the Multiple Selection check box is selected, multiple visits can be selected and signed out at once. Selecting this option does the same thing as clicking the [Sign Out] button. To use this feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the General Cardholder Options form of the Cardholder Options folder. For more information, refer to Configure System-wide Visit Options on page 445.

When selected, the actual **Time out** for the visit is updated to the current date/time.

If the visitor has an active badge, the deactivate date is updated and the badge status is set to the status setup that was selected on the General Cardholder Options form.

Find Cardholder

Opens the Cardholders folder and displays the cardholder record that is associated with the currently selected visit.

Find Visitor

Opens the Cardholders folder and displays the visitor record that is associated with the currently selected visit.

Refresh

Click this button to refresh the visits listed in the Visits listing window. When someone else makes changes in the database, you may need to click this button to see the changes. (Cardholder information is not automatically updated, but visit information is.)

Visits Folder Fields

Visits listing window

Displays the status, host, visitor, scheduled time in, scheduled time out, time in, time out, visit type and visit purpose for visit records.

Host name

Specifies the host for whom you want to display scheduled visits.

Visitor name

Specifies the visitor for whom you want to display scheduled visits.

Status

Displays the status of the visit. Choices include:

- **Scheduled** - A visit that has a scheduled time in and scheduled time out that are both in the future
- **Late** - A visit where the current date and time is after the scheduled time in
- **Overstayed** - A visit where the current date and time is after the scheduled time out

- **Active** - A visit that has been signed in and the scheduled time out has not yet been reached
- **Finished** - A visit occurred in the past and has been signed out

Search

Allows you to search based on any field on any form in the Visits folder. The search results will be displayed in the Visits listing window.

Add

Allows you to add a visit record.

Modify

Allows you to modify a selected visit record. Multiple selection cannot be used when modifying visit records. If the **Multiple Selection** check box is selected and multiple visit records are selected, the [Modify] button will be grayed out.

Delete

Allows you to delete a selected visit record. If the **Multiple Selection** check box is selected, multiple visit records can be deleted at once. The visit(s) will be deleted without prompting for confirmation.

Print

Allows you to print a disposable badge. Disposable badge types are configured in the Badge Types folder. For a badge type to be used to print disposable badges, it must have “Visitor” selected for the **Class** and the **Disposable** check box must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

Sign In

If selected, the Sign In Visit(s) window is displayed. In this window, select whether to print disposable badges for the visitor(s) that are being signed in. If the **Multiple Selection** check box is selected, multiple visit records can be signed in at once.

Sign Out

To use this feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the General Cardholder Options form of the Cardholder Options folder. For more information, refer to Configure System-wide Visit Options on page 445.

When selected, the actual **Time Out** for the visit is updated to the current date/time.

If the visitor has an active badge, the deactivate date is updated and the badge status is set to the status setup that was selected on the General Cardholder Options form.

Multiple Selection

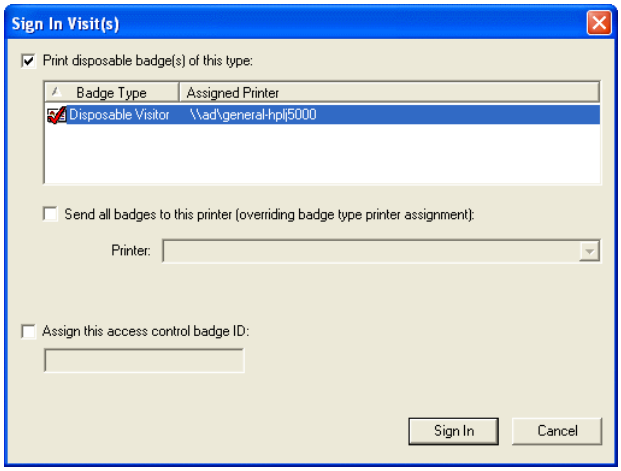
If selected, more than one entry in the listing window can be selected simultaneously. The changes made on this form will apply to all selected visits. This feature is primarily used for printing badges, signing in visits and signing out visits.

Sign In Visit(s) Window

This window is displays when:

- A visit is added in the Visits folder and the **Sign In Now** check box is selected on the Visit form.
- A visit record is selected in the Visit listing window in the Visits folder and the [Sign In] button is clicked.

- Automatic sign in is enabled. For more information about this feature, refer to the Automatic Sign In section of the Visitor Management User Guide.



Print disposable badge(s) of this type

For this field to be enabled, the **Allow disposable badge printing** check box on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. Displays a list of disposable badge types that can be selected for the visit. Only those badge types that are disposable are listed. If you do not want to print a disposable badge for the visitor, deselect this check box.

Send all badges to this printer (overriding badge type printer assignment)

Select this check box to select an alternate printer. For these fields to be enabled, the user must have be rights to access to the **Choose alternate printer** option via the Users Folder, Cardholder Permission Groups Form. For more information, refer to Cardholder Permission Groups Form on page 364. Selecting this check box overrides the printer assignments in the Printing/Encoding form of the Badge Types folder.

Assign this access control badge ID

For this field to be enabled, the **Allow access control badge assignment** check box on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. The badge must already exist in the system The existing badge's class must be "Visitor." If the visitor already has an active access control badge (from a manual assignment or another visit), this field will automatically be populated with that ID. If you do not want to assign an access control badge ID for the visitor, deselect this check box.

Sign In

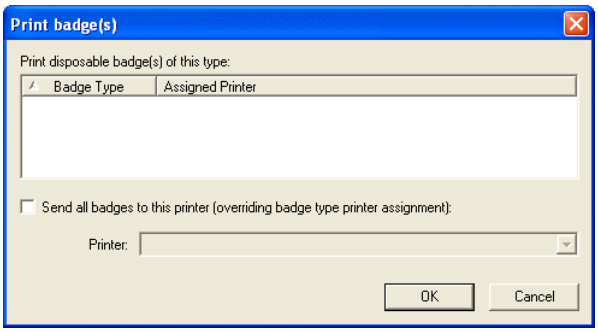
Signs in the visit using the options selected on the form.

Cancel

Closes the Sign In Visit(s) window without signing in the visit.

Print Badge(s) Window

This window displays when the [Print] button is clicked on any form in the Visits folder.



Print disposable badge(s) of this type

For this field to be enabled, the **Allow disposable badge printing** check box on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. Displays a list of disposable badge types that can be selected for the visit. You must select a badge type and only one badge type can be selected. Only those badge types that are disposable are listed.

Send all badges to this printer (overriding badge type printer assignment)

Select this check box to select an alternate printer. Chose the printer from the drop-down list. For these fields to be enabled, the user must have access rights to the **Choose alternate printer** option via the Users Folder, Cardholder Permission Groups Form For more information, refer to Cardholder Permission Groups Form on page 364. Selecting this check box overrides the printer assignments in the Printing/Encoding form of the Badge Types folder.

OK

Prints the disposable badge.

Cancel

Closes the Print Badge(s) window without printing the visit.

Visits Folder Procedures

The following procedures pertain to every form in the Visits folder unless otherwise noted.

Visit Search Capabilities

In search mode, you can search on any combination of fields in the Visits folder, including the Status search, Visit and Details forms. On the E-mail and Reports forms, you can only search for the host name or visitor name.

Comparison Operators

Comparison operators are symbols that represent specific actions. You can refine your search by prefixing search fields with a comparison operator. Refer to the following table to identify the comparison operators you can use with different fields.

Comparison operator	Description	Text field	Numeric field	Drop-down list
=	Equal to	Yes	Yes	Yes
!= or <>	Not equal to	Yes	Yes	Yes
>	Greater than	Yes	Yes	NA
<	Less than	Yes	Yes	NA
>=	Greater than or equal to	Yes	Yes	NA
<=	Less than or equal to	Yes	Yes	NA
%	Contains	Yes	NA	NA

Notes: "Equal to" is the default comparison operator for numeric and drop-down list fields.

If you type an equal to sign "=" in a field and nothing else, OnGuard will search for records that have an empty value for that field. For example, typing an "=" in the Department field will find every record that does not have an assigned department.

Search Fields Using "Begins With"

For text and drop-down list fields you can search records whose values begin with specific characters by entering those characters in the field. For example, when searching by last name, a filter of "L" will find "Lake", "Lewis", etc. A filter of "Lake" will find "Lake", "Lakeland", etc.

Note: The default comparison operator for text fields is "begins with".

Search Multiple Fields

When you search multiple fields, the search criteria for each field is combined. For example, typing "A" in **Last name** field and "B" in **First name** field will find all people whose last name begins with "A" and whose first name beings with "B".

One exception is searching access levels, which uses an "or" comparison for multiple selections. For example, selecting both "Access Level A" and "Access Level B" will find all cardholders with either "Access Level A" or "Access Level B" assigned.

Note: If you want to search for a range of Badge IDs, take advantage of the two Badge ID fields on the Badge form. One field is located in the middle-left section of the form and the other field is located in the right section of the form. Note, the form must be in modify mode to see both fields. Type ">= 100" in one field and "<= 200" in the other to find all badges with IDs between 100 and 200 (inclusive).

Search for All Visits to a Selected Cardholder

This procedure will search for every person who visited a selected cardholder.

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. On the Visit tab, click [Search].
3. Do one of the following:
   - Enter the full or partial last name of the cardholder in the **Host name** drop-down list.
   - Use the Select Host Wizard by leaving the **Host name** drop-down list blank and clicking the [...] button to the right it. When the wizard opens, enter any information that you know about the cardholder and click [Next]. The wizard will display all records that match the criteria you entered. Select the correct cardholder and click [Finish].
4. Click [OK]. OnGuard displays all the visits made to the selected cardholder. If you entered a partial cardholder name, OnGuard displays all the visits made to the cardholders that meet the search criteria.

Search for All Visits by a Selected Visitor

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. On the Visit tab, click [Search].
3. Do one of the following:
   - Enter the full or partial last name of the visitor in the **Visitor name** drop-down list.
   - Use the Select Host Wizard by leaving the **Visitor name** drop-down list blank and clicking the [...] button to the right it. When the wizard opens, enter any information that you know about the visitor and click [Next]. The wizard will display all records that match the criteria you entered. Select the correct visitor and click [Finish].
4. Click [OK]. OnGuard displays all the cardholders the selected visitor has met with. If you entered a partial visitor name, OnGuard displays all the cardholders visited by the visitors that meet the search criteria.

Search for Scheduled, Active or Finished Visits

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. On the Status search tab, click [Search].
3. In the Search for visits section, select that status you wish to search for.
   - To search for scheduled visits, select the **Scheduled, future** check box.
     - If you wish to search for visits that are scheduled to begin in a specified amount of time, select the **Starting within** check box and specify the number of minutes, hours, or days.
     - By default, scheduled visits that are late getting started are included in the search. If you do not want to search for scheduled visits that are late, deselect the **Scheduled, late** check box.
   - To search for active visits, select the **Active** check box.
     - If you wish to search for visits that are scheduled to end within a specified amount of time, select the **Ending within** check box and specify the number of minutes, hours, or days.
     - By default, active visits that are late signing out (overstayed) are included in the search. If you do not want to search for overstayed visits, deselect the **Active, overstayed** check box.
   - To search for finished visits, select the **Finished** check box.
4. The refresh rate is how often (in minutes) the database is queried for changes.
   - Select the **Use system default rate** check box to use the system default rate. Notice the **Refresh rate** field automatically populates with the default value.

- Deselect the **Use system default rate** check box to use a different rate. Enter the new rate in the **Refresh rate** field. This setting is stored on a per user basis.

5. Click [OK]. The visit records that meet the search criteria display in the Visits listing window.

Search for All Visits for a Specific Date or Time

Depending on the fields you populate, this procedure will search for:

- Visits scheduled to start on a specific date or time.
- Visits scheduled to end on a specific date or time.
- Visits that start on a specific date or time.
- Visits that end on a specific date or time.

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. On the Visit tab, click [Search].
3. To search for a specific date:
   a. Click the [...] button to the right of one of the four date fields (Scheduled time in, Scheduled time out, Time in, or Time out). The Select Date(s) window opens.

   b. Complete one of the following:
      - Select a time range and the number of days to search. If you select “Today”, you do not need to enter the number of days to search.
      - Select a time range and a date.
      - Select a start date and the number of days to search.
      - Select a start date and end date.
   c. Click [OK]. The code for the search criteria that you specified displays in the Visit form.
4. To search for a specific time:
   a. Click the [...] button to the right of one of the four time fields. The Select Time Range window opens.

   b. Select the start time range and enter a time.
   c. Select the end time range and enter a time.

Notes: If you select “None” for a time range, you cannot enter a specific time.

You can change the time by using the spin buttons or typing new values. The hour, minute, and time of day are adjusted individually.

   d. Click [OK].
5. Click [OK] on the Visit form. The visit records that meet the search criteria display in the listing window.
6. Repeat steps 3-5 to search for scheduled time in, scheduled time out, time in, or time out.

Retrieve the Most Recent Visit Search Results

1. Display the Cardholders folder or Visits folder by completing one of the following:
   - To display the Cardholders folder in Alarm Monitoring, select ***Badge Info*** from the ***View*** menu. For all other applications, select ***Cardholders*** from the ***Administration*** menu.
   - To display the Visits folder in Alarm Monitoring, select ***Visits*** from the ***View*** menu. For all other applications, select ***Visits*** from the ***Administration*** menu.
2. Click [Search].
3. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
4. You can optionally modify your search criteria.
5. Click [OK].
6. OnGuard retrieves and displays the first matching record. Use the navigational buttons to look at additional matching records.

Find a Cardholder or Visitor Associated with a Visit

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. Locate the visit record that you wish to find the visitor or cardholder for.
3. Right-click on the visit record.
   - If you wish to view the cardholder record, select **Find Cardholder**.
   - If you wish to view the visitor record, select **Find Visitor**.
4. The record of the corresponding cardholder or visitor will be displayed in the Cardholder or Visitor window.

Add a Visit Record

To add a visit, information about the visit needs to be entered on the Visit, Details and E-mail forms in the Visits folder; it does not matter which form you start with. When the Visits folder opens, the Visit form displays by default, so this procedure begins on that form.

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. On the Visit form:
   a. A new visit record can either be based on an existing visit record or it can be an entirely new record.
      - To create a record based on an existing visit record, select a visit record in the Visits listing window, then click [Add]. The fields prepopulate with the information from the selected visit. You can select new values for any field.
      - To create a record that is not based on an existing visit record, make sure that no visit record is selected in the Visits listing window, then click [Add]. The fields will be blank to begin with.

Note: Steps b and c can be done in either order.

   b. Click the [...] button to the right of the **Host name** drop-down list. The Select Host Wizard: Search form opens. For more information, refer to Select Host Wizard: Search Form on page 168.
      1) Specify your search criteria by typing full or partial entries in the enabled fields.

Note: Leave all fields blank to display all cardholders.

2) If a visitor is specified and you wish to search for only cardholders who have been visited by that visitor, select the **Previous hosts for current visitor only** check box.
3) Click [Next].
4) The Select Host Wizard: Select form opens. In the Cardholder listing window, select the cardholder you wish to add a visitor for. For more information, refer to Select Host Wizard: Select Form on page 170.
5) Click [Finish]. The cardholder's name appears in the **Host name** field on the Visit form.

c. Click the [...] button to the right of the **Visitor name** field. The Select Visitor Wizard: Search form displays.
1) Specify your search criteria by typing full or partial entries in the enabled fields.

Note: Leave all fields blank to display all visitors.

2) If a cardholder is specified and you wish to only search for visitors who have visited that cardholder, select the **Previous visitors for current host only** check box.
3) Click [Next].
4) The Select Visitor Wizard: Select or Add form displays. If the Visitor is listed below, select the visitor and click [Finish]. The visitor's name appears in the **Visitor name** field on the Visit form. If the Visitor is not listed below, select the **Create new visitor** radio button and click [Next]. The Select Visitor Wizard: Add form displays. Enter the new visitor's information and click [Finish].

Note: For a detailed description of the Select Visitor Wizard: Select or Add form refer to Select Visitor Wizard: Select or Add Form on page 172.

d. In the **Scheduled time in** fields, specify the date and time the visit will begin. You can either type the values or select them.

Note: If the **Sign In Now** check box is selected, these fields will be grayed out.

e. In the **Scheduled time out** fields, specify the date and time the visit will end. You can either type the values or select them.
f. Select the **Sign In Now** check box if the visit is starting immediately. If you select this option, the **Scheduled time in** fields will become grayed out and the date and time when you click the [OK] button will be assigned as the visit's **Time in**.

3. Click the Details tab. For a detailed description of the Details form refer to Details Form on page 163. On the Details form:
a. In the **Type** drop-down list, select the type of visit.

Note: Types of visits must first be configured in the List Builder, which is displayed by selecting the ***Administration*** menu, then selecting ***List Builder***. For more information, refer to Chapter 19: List Builder Folder on page 481.

b. In the **Purpose** field, type the reason for the visitor's visit.

4. You may wish to send e-mail notifications to all parties that require information about a scheduled visit. For a detailed description of the E-mail form refer to E-mail Form on page 164. To set up e-mail notifications, click the E-mail tab. On the E-mail form:

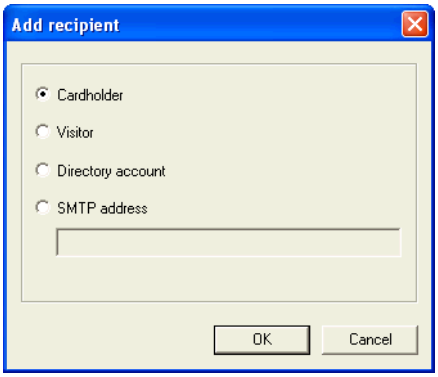
Note: For an e-mail to be sent, the **Allow e-mail notification** check box on the Visits form in the Cardholder Options folder must be selected.

a. In the Include section, verify the **Default Recipients** check box is selected as long as you wish to send e-mail messages to the default recipients. The default recipients are configured in the following locations:
   - On segmented systems, select Administration > Segments, click the Segments tab, then click the Visits sub-tab. On the Visits sub-tab, you can view or modify the default recipients.
   - On nonsegmented systems, select Administration > System Options, then click the Visits tab. On the Visits tab, you can view or modify the default recipients.

b. Select the **Cardholder for this visit** check box if you wish to have an e-mail sent to the cardholder for this visit.

c. Select the **Visitor for this visit** check box if you wish to have an e-mail sent to the visitor for this visit.

d. Click [Add] if you wish to add another recipient. The Add recipient window displays. You may add a cardholder, visitor, directory account or SMTP address.

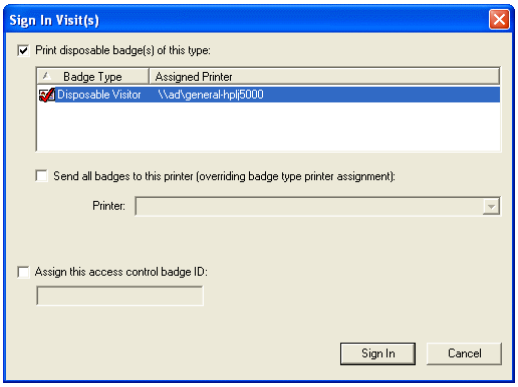


   - If you select the **Cardholder** radio button and click [OK], the Select Host Wizard: Search form displays. For a detailed description of the Select Host Wizard: Search form refer to Select Host Wizard: Search Form on page 168.
   - If you select the **Visitor** radio button and click [OK], the Select Visitor Wizard: Search form displays. For a detailed description of the Select Visitor Wizard: Search form refer to Select Visitor Wizard: Search Form on page 171.
   - If you select the **Directory account** radio button and click [OK], the Select Account window displays.
   - If you select the **SMTP address** radio button, type the SMTP address, then click [OK]. An example of an SMTP address is “joesmith@company.com”.

5. Click [OK].

6. If the **Sign in now** check box was selected, proceed to step 7. If the **Sign in now** check box was not selected, the visit will be added. The value for the **Time In** column for the visit will remain blank and the visit can be signed in later when it actually occurs.

7. If none of the **Allow disposable badge printing**, **Allow access control badge assignment** and **Allow e-mail notification** check boxes are checked on the Visits form in the Cardholder Options folder, the visit will be signed in. If any of those options are selected, the Sign In Visit(s) window displays.



8. The **Print disposable badge(s) of this type** check box and listing window are enabled if the **Allow disposable badge printing** check box is selected on the Visits form in the Cardholder Options folder.
   - If enabled, you can print a disposable badge for the user by selecting the **Print disposable badge(s) of this type** check box, then selecting a disposable badge type to be assigned and printed.

Note: Disposable badge types are configured in the Badge Types folder. For a badge type to be used to print disposable badges, it must have "Visitor" selected for the **Class** and the **Disposable** check box must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

   - If the check box is deselected, the system will not print a disposable badge.
9. To override the badge type printer assignment select the **Send all badges to this printer (overriding badge type printer assignment)** check box and select the printer from the drop-down list. This check box and drop-down list are enabled if the **Print disposable badge(s) of this type** check box is selected and the user has the correct permissions.
10. The **Assign this access control badge ID** check box and field are enabled if the **Allow access control badge assignment** check box is selected on the Visits form in the Cardholder Options folder.
    - If enabled, you can select the **Assign this access control badge ID** check box and then type the number of an existing badge that has the class "Visitor" in the field or leave the field blank.
    - If the visitor already has an active access control badge (from manual assignment or another visit), this field will automatically be filled in with that ID.
    - If the check box is deselected, the system will not attempt to assign an access control badge ID.
11. Click [Sign In]. The visit will be added, the **Time In** field will be updated to the current date and time and any access control badge assigned will become active.

Modify a Visit Record

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. Locate the visit record you want to change and select it in the Visits listing window.

Note: Multiple selection cannot be used when modifying visits.

3. Click [Modify].
4. Make the changes you want to the record. Changes can be made on any tab in the Visits folder.

5. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Visit Record

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. In the Visits listing window select the visit record you want to delete.

Note: To select multiple visit records select the **Multiple Selection** check box.

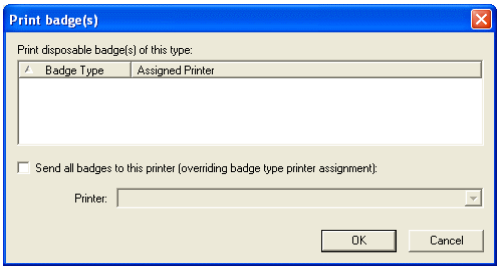
3. Click [Delete].
4. Click [OK]. The visit(s) will be deleted without confirmation.

Print a Visitor Badge

1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. In the Visits listing window select the visit record you want to print.

Note: To select multiple visit records select the **Multiple Selection** check box.

3. On any form in the Visits folder, click [Print].
4. The Print badge(s) window displays. In the **Print disposable badge(s) of this type** listing window select the type of badge to print.



Note: Disposable badge types are configured in the Badge Types folder and must have "Visitor" selected for the **Class** and the **Disposable** check box selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

5. To select an alternate printer select the **Send all badges to this printer (overriding badge type printer assignment)** check box and choose a printer from the drop-down list. This check box and drop-down list are enabled if the user has the correct permissions.
6. Click [OK].

Sign in a Previously Scheduled Visit and Print a Badge

Each visit has a time that it is scheduled to begin. When the visitor arrives and the visit actually begins, the visit should be "signed in". When a visit is signed in, the actual **Time In** of the visitor is updated to the current date and time and any access control badge that the visitor is issued is activated. A visit can be signed in immediately after it is added or it can be signed in later.

1. Open the Sign In Visit(s) dialog by completing one of the following:
   a. Add a visit. For more information, refer to Add a Visit Record on page 154.
   b. Search for an existing visit and click [Sign In]. For more information, refer to Search for Scheduled, Active or Finished Visits on page 152.

2. Depending on how the badge types are configured, different fields are active on the Sign In Visit(s) form.
   - To print a disposable visitor's badge using the default printer assignment, complete steps 1 and 4 (below).
   - To print a disposable visitor's badge by overriding the default printer assignment, complete steps 1, 2, and 4.
   - To print a non-disposable visitor's badge by using the default printer assignment, complete steps 3 and 4.
   - To print a non-disposable visitor's badge by overriding the default printer assignment, complete steps 1 through 4.
     1) Select the Print disposable badge(s) of this type check box and select a badge type.
     2) Select the Send all badges to this printer (overriding badge type printer assignment) check box and select the printer from the drop-down list.
     3) Select the Assign this access control badge ID check box and enter the badge ID. Note, the badge ID must exist in the database as an active visitor badge ID. If the visitor already has an active access control badge, this field will automatically be filled in with that ID.
     4) Click [Sign In].

Note: Disposable badge types are configured in the Badge Types folder. For a badge type to be used to print disposable badges, it must have "Visitor" selected for the **Class** and the **Disposable** check box must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

Sign Out a Visit

Each visit has a time that it is scheduled to end. When the visitor leaves and the visit actually ends, the visit should be "signed out." When a visit is signed out, the actual **Time Out** of the visitor is updated to the current date and time and any access control badge that the visitor is issued is deactivated.

To use the Sign Out feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the Visits form in the Cardholder Options folder. For more information, refer to Configure System-wide Visit Options on page 445.

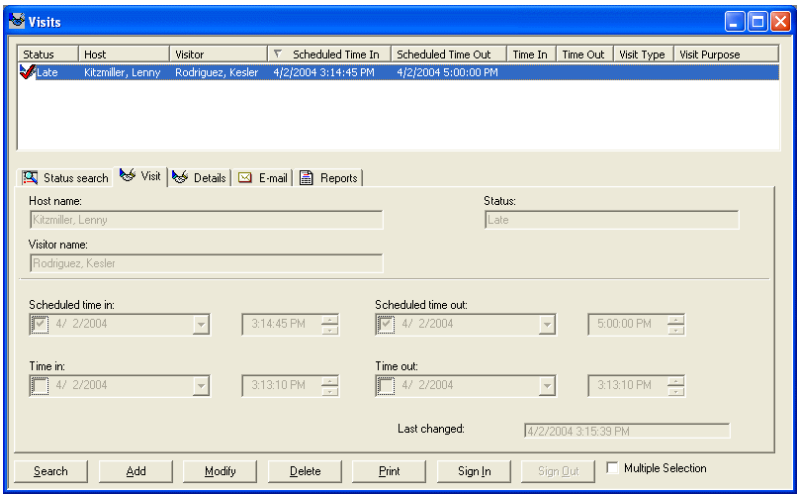
1. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
2. Locate the active visit record that needs to be signed out.
3. In the Visits listing window, select the active visit that you want to sign out by clicking on it.
4. Click [Sign Out].
5. The message "Are you sure you wish to sign out the selected visit(s)? This will also deactivate any badges the visitors have." will be displayed. Click [Yes] to complete the sign out. The **Time out** will be updated to the current date/time. If the visitor has an active badge, the deactivate date will be updated and the badge status will be set to the status setup that was selected on the Cardholder Options form. The signed out visit will appear in the Visits listing window.

Visit Form

The Visit form is displayed by default when the Visits folder opens. It is used to:

- Add or modify visits

- Display visit records for a selected date range
- Search for visit records based on the scheduled time in, scheduled time out, time in, time out or date and time last changed



Scheduled time in

Select the date and time that the visit is expected to start.

Time in

When a visit is signed in, the visit's **Time in** gets updated to the current date and time.

Scheduled time out

Select the date and time that the visit is expected to end.

Time out

When a visit is signed out, the visit's **Time out** gets updated to the current date and time.

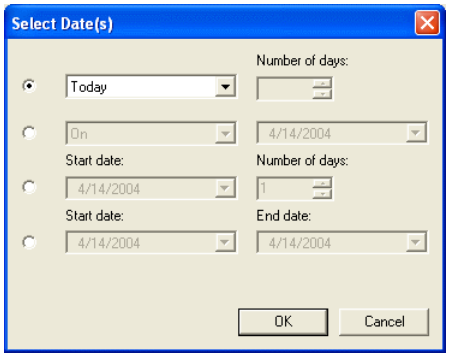
Last changed

Indicates the date and time on which this visit record was last modified and saved.

This date and time are only updated when visit information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

Select Date(s) Window

This window is only displayed when the Visit form in the Visits folder is in Search mode. In Search mode, click the [...] button to the right of the first **Scheduled time in**, **Time in**, **Scheduled time out** or **Time out** field.



Day

Used when searching for a scheduled time in, time in, scheduled time out or time out. Selects visits that occurred today, on a previous number of days or on a specified number of days in the future.

Specific Date

Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects visits that occurred on a specified date. Choices include on, on or after, after, on or before or before a specified date.

Number of Days After a Date

Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects visits between a specified start date and a specified number of days after the start date.

Between Two Dates

Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects all visits that occurred between the specified Start date and the End date.

OK

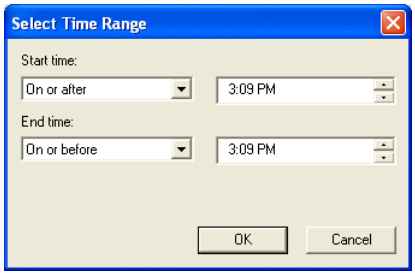
Enters the code for the selected search criteria in the respective field on the Visit form in the Visits folder.

Cancel

Closes the Select Date(s) window without selecting a date search criteria.

Select Time Range Window

This window is only displayed when the Visit form in the Visits folder is in Search mode. In Search mode, click the [...] button to the right of the second **Scheduled time in**, **Time in**, **Scheduled time out** or **Time out** field.



Start time

Used when searching for the time portion of a scheduled time in, time in, scheduled time out or time out. Allows you to search for visits that start on or after or after a specified time. If “None” is selected, no time restraints are put on the visit records that are returned. (Visits that started at any time on the specified date will be returned.)

End time

Used when searching for the time portion of a scheduled time in, time in, scheduled time out or time out. Allows you to search for visits that end on or before or before a specified time. If “None” is selected, no time restraints are put on the visit records that are returned. (Visits that ended at any time on the specified date will be returned.)

OK

Enters the code for the selected search criteria in the respective field on the Visit form in the Visits folder.

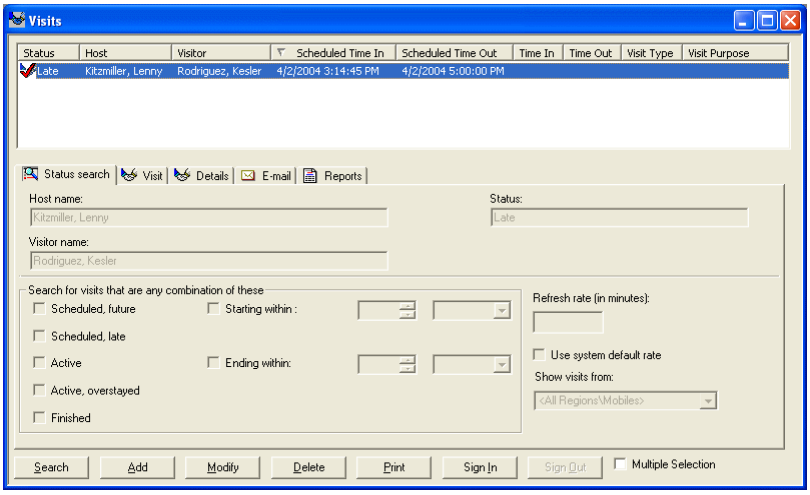
Cancel

Closes the Select Time Range window without selecting a time search criteria.

Status Search Form

The Status Search form is only enabled when the [Search] button is clicked. It is used to:

- Search for Visits that meet a specified criteria (scheduled in the future, scheduled but late, active, finished, etc.)
- Set the refresh rate



Scheduled, future

If selected, the search will find visits that are scheduled in the future, i.e., have a scheduled time in that is in the future and have not been signed in yet

Starting within

Enabled for selection only when the **Scheduled, future** check box is selected. If selected, specify the number of hours, days or minutes that the visit is scheduled to begin in. For example, you can search for all visits that are scheduled to begin within the next two days.

Scheduled, late

If selected, the search will find visits that are late, i.e., have a scheduled time in that is in the past and have not been signed in yet

Active

If selected, the search will find all visits that are currently signed in and have not been signed out yet

Ending within

Enabled for selection only when the **Active** check box is selected. If selected, specify the number of hours, days or minutes that the visit is scheduled to end in. For example, you can search for all visits that are scheduled to end within the next two days.

Active, overstayed

If selected, the search will find all visits that are currently signed in where the current date and time is after the scheduled time out. For example, a visitor that was supposed to leave at 3 p.m., but is still visiting at 5 p.m.

Finished

If selected, the search will locate visits that occurred in the past.

Refresh rate (in minutes)

The refresh rate is how often the database is queried to see if it has changed. The refresh rate is stored on a per user basis and only applies when searching based on a status (i.e., the “Scheduled, future”, “Scheduled, late”, “Active”, “Active, overstayed” or “Finished” status) on the Status search form in the Visits folder. The default value is set in the **Refresh rate (in minutes)** field on the Visits form in the Cardholder Options form. A custom refresh rate can be specified as long as the **Use system default rate** check box is not selected.

Use system default rate

If selected, the system default rate will be used when refreshing. The system default rate is set in the **Refresh rate (in minutes)** field on the Visits form in the Cardholder Options folder.

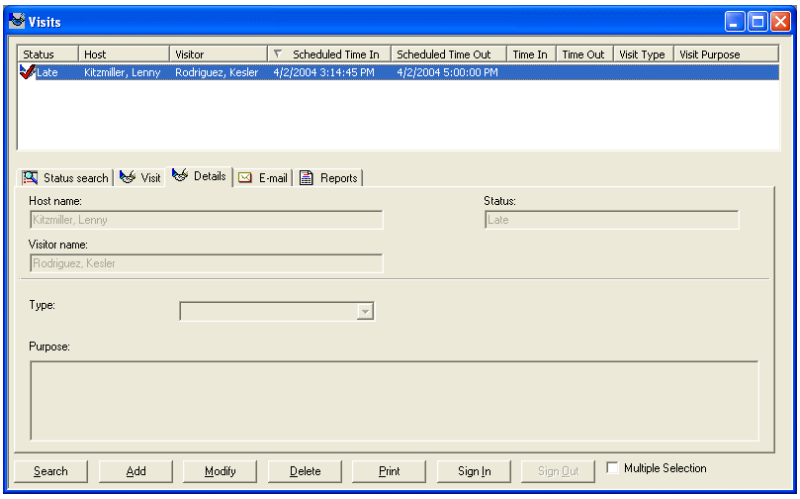
If not selected, a custom refresh rate can be specified in the **Refresh rate (in minutes)** field.

Show visits from

For Enterprise systems only: From this drop-down, select a server node (Regional or Master) or a mobile station from which to display visits. Alternatively, select "<All Regions\Mobiles>" to display visits from all server nodes and mobile stations. When a visit is added, in order for it to be displayed at another server node or mobile station, replication must be performed at the computer where the visit was added.

Details Form

The Details form is a user-defined form that has been created for you. This form can be modified or even deleted using FormsDesigner. By default, the form contains the type and purpose of the visit.



Type

Select the type of visit.

Types of visits must first be configured in the List Builder, which is displayed by selecting the ***Administration*** menu, then selecting ***List Builder***. For more information, refer to Chapter 19: List Builder Folder on page 481.

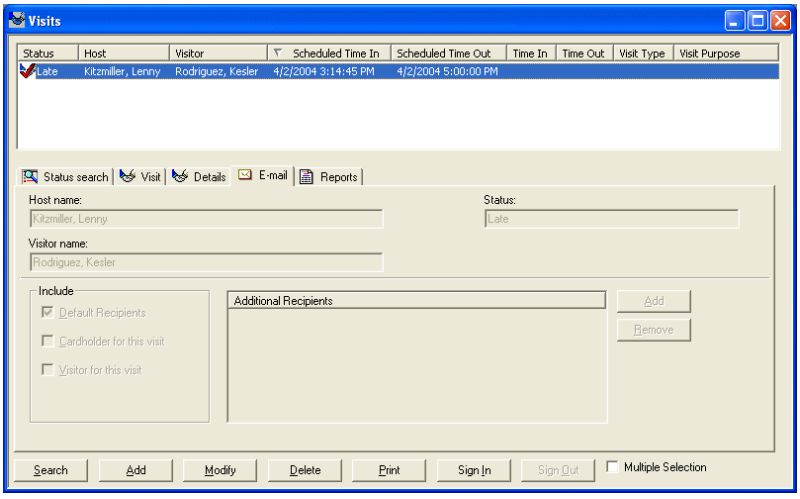
Purpose

Type the reason why the visitor is visiting the cardholder.

E-mail Form

The E-mail form is used to specify e-mail addresses and pager numbers that are automatically notified of visits. You can:

- Add a recipient
- Remove a recipient
- Specify whether to e-mail the default recipients, the cardholder being visited and/or the visitor



Default Recipients

Select this check box if you wish to send e-mail messages to the default recipients.

On segmented systems, select Administration > Segments, click the Segments tab, then click the Visits sub-tab. On the Visits sub-tab, you can add or remove recipients. These recipients will be collectively considered the “Default Recipients” on the E-mail form in the Visits folder.

On non segmented systems, select Administration > System Options, then click the Visits tab. On the Visits tab, you can view or modify the default recipients.

Whether this check box is selected by default when a new visit is added is determined by the **Include default recipients by default** check box on the Visits form in the Cardholder Options folder.

Cardholder for this visit

Select this check box if you wish to have an e-mail sent to the cardholder for this visit. Whether this check box is selected by default when a new visit is added is determined by the **Include host’s e-mail by default** check box on the Visits form in the Cardholder Options folder.

Visitor for this visit

Select this check box if you wish to have an e-mail sent to the visitor for this visit. Whether this check box is selected by default when a new visit is added is determined by the **Include visitor’s e-mail by default** check box on the Visits form in the Cardholder Options folder.

Additional Recipients listing window

Displays the e-mail addresses that will receive e-mail notification of visits. The addresses for the default recipients are not displayed in this listing window.

Add

Click this button if you wish to add another recipient. The Add recipient window is displayed. You may add a cardholder, visitor, directory account or SMTP address.

If you select the **Cardholder** radio button and click [OK], the Select Host Wizard: Search form is displayed.

If you select the **Visitor** radio button and click [OK], the Select Visitor Wizard: Search form is displayed.

If you select the **Directory account** radio button and click [OK], the Select Account window is displayed.

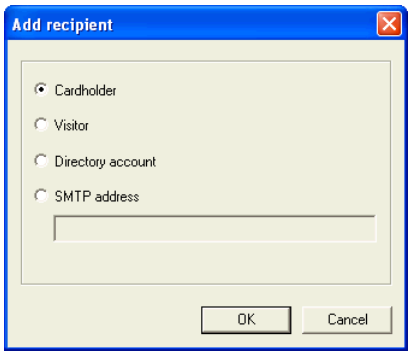
If you select the **SMTP address radio button**, type the SMTP address, then click [OK]. An example of an SMTP address is “joesmith@company.com”.

Remove

Removes the selected recipient from the list of recipients that will receive notification of visits.

Add Recipient Window

This window is displayed when the E-mail form in the Visits folder is in Add or Modify mode and the [Add] button to the right of the Additional Recipients listing window is clicked.



Cardholder

The Select Host Wizard: Search form is displayed, which allows you to add a cardholder as an e-mail recipient. For more information, refer to Select Host Wizard: Search Form on page 168.

Visitor

The Select Visitor Wizard: Search form is displayed, which allows you to add a visitor as an e-mail recipient.

Directory account

The Select Account window is displayed, which allows you to add a directory account as an e-mail recipient.

SMTP address

Type the SMTP address, then click [OK]. An example of an SMTP address is "joesmith@company.com".

OK

If you selected the **Cardholder** radio button, the Select Host Wizard: Search form is displayed. For more information, refer to Select Host Wizard: Search Form on page 168.

If you selected the **Visitor** radio button, the Select Visitor Wizard: Search form is displayed. For more information, refer to Select Visitor Wizard: Search Form on page 171.

If you selected the **Directory account** radio button, the Select Account window is displayed.

If you selected the **SMTP address** radio button and typed an SMTP address, the address will be added to the Additional Recipients listing window.

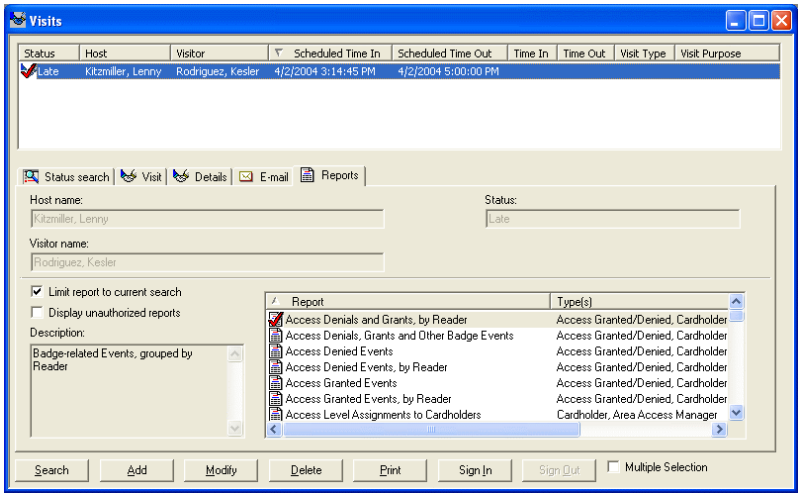
Cancel

Closes the Add recipient window without adding a recipient.

Reports Form

The Reports form shows only visit-related reports. On the Reports form you can:

- Search for a cardholder
- Search for a visitor
- Generate a report



Limit report to current search

If selected, the report will only include those records that match the rest of the search criteria specified on any form in the Visits folder. If not selected, the report will include all records for the selected report type.

Display unauthorized reports

By default, the visits report tab only lists reports that users have permissions to preview. If the **Display unauthorized reports** check box is selected, reports that are disabled for a user will appear in the report listing window. The user can identify which reports are disabled by whether the [Print] button is inactive. This allows the user to ask the system administrator for permission to an existing report, if desired.

Reports are authorized and unauthorized by using report permission groups. For more information, refer to Report Permission Groups Form on page 371.

Description

A brief description of the report contents.

Report listing window

Lists currently defined reports of the type(s) selected in the Report listing window.

Reports Form Procedures

The following procedures can be performed on this form.

Run a Visit Report from the Visits Folder

A visit report can be generated for either a defined search criteria or for all visits.

1. If you wish to generate a visit report that searches through all visit records not just those that match a search criteria, proceed to step 2. To generate a visit report based on a search criteria:
   a. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
   b. In the Visits folder, click [Search].

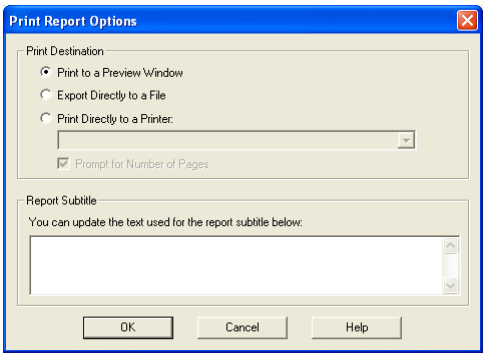
c. Run the search that you wish to print a report for. For more information on searching refer to the following:
   - Visit Search Capabilities on page 150
   - Search for All Visits to a Selected Cardholder on page 151
   - Search for All Visits by a Selected Visitor on page 152
   - Search for Scheduled, Active or Finished Visits on page 152
   - Search for All Visits for a Specific Date or Time on page 153
   - Retrieve the Most Recent Visit Search Results on page 154

d. Click the Reports tab.

e. Select the **Limit report to current search** check box.

f. Proceed to step 3.

2. To generate a visit report that searches through all visits:
   a. Select ***Visits*** from the ***Administration*** menu. The Visits folder opens.
   b. In the Reports listing window, select the type of report you wish to print.
   c. Proceed to step 3.
3. Click [Print]. The Print Report Options window opens.



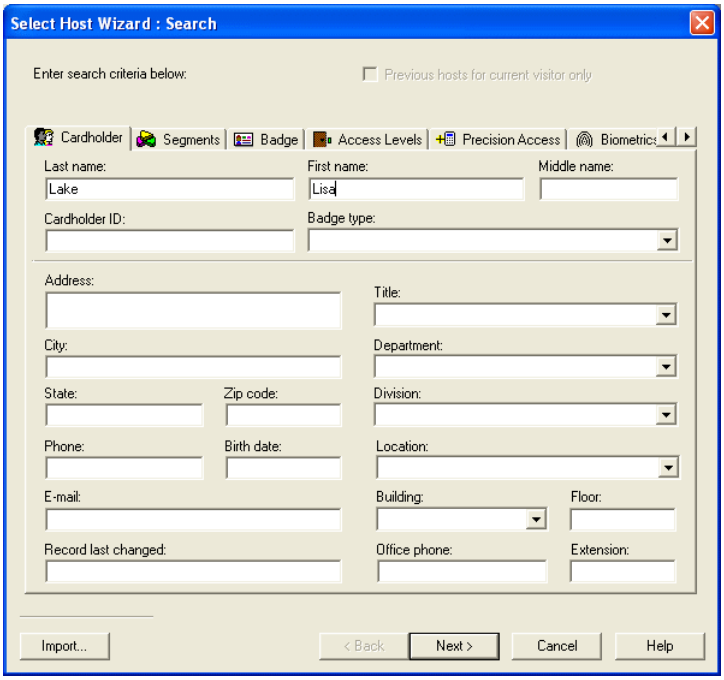
4. In the Print Destination section, select whether to print to a preview window, export directly to a file or print directly to a printer.
5. If you selected **Print Directly to a Printer** in the Print Destination section, select a printer in the drop-down list and choose whether to **Prompt for Number of Pages**.
6. In the Report Subtitle section, type the report subtitle. If the **Limit report to current search** check box is selected, the search criteria will be listed in the Report Subtitle section by default. The subtitle will be displayed below the report title on the report.
7. Click [OK]. The options selected in the Print Destination section will determine where the report is sent.

Select Host Wizard: Search Form

This form is used to enter search criteria that will allow you to locate a specific cardholder.

Note: If the FormsDesigner application has been used to customize your cardholder data, the elements on your Select Host Wizard: Search form will be different. The default fields are pictured below.

This form is displayed when the [Search] button in the Visits folder is clicked and then the [...] button to the right of the **Host name** field is clicked.



Previous hosts for current visitor only

This check box is only enabled when a visitor has been selected and a cardholder is being searched for. If selected, only those cardholders who have previously been visited by the selected visitor will be displayed on the Select Visitor: Select or Add form.

Last name

Indicates cardholder's last name.

First name

Indicates cardholder's first name.

Middle name

Indicates cardholder's middle name.

Cardholder ID

Indicates a cardholder's ID, which is most commonly their Social Security Number. The cardholder ID must be a numeric value.

Badge type

Selects which of the cardholder's badges (if he or she has more than one) is to be the active one.

User-defined fields

All fields below the line on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your cardholder data.

Back

This button is not used.

Next
The wizard will proceed to the Select Host Wizard: Select form.

Cancel
Closes the window without locating a cardholder and returns you to the Visit form in the Visits folder.

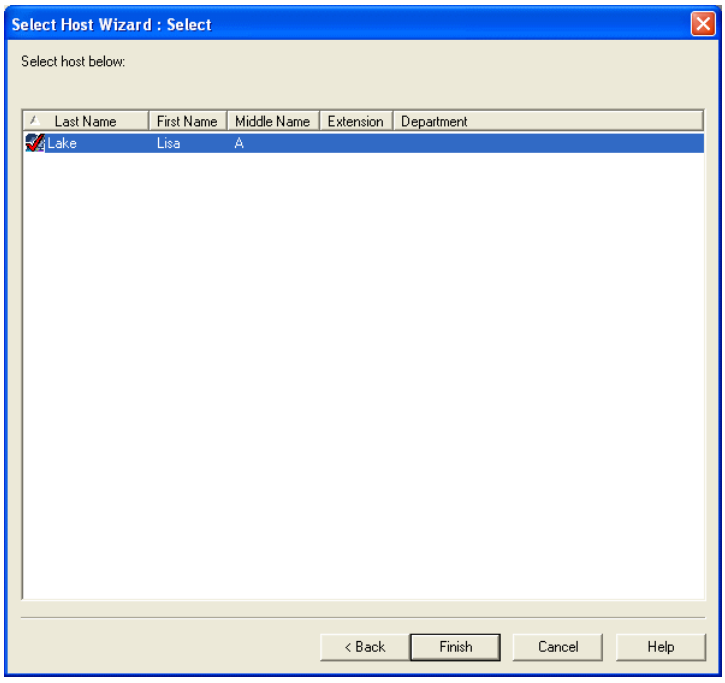
Help
Displays online help for this topic

Import
Displays the Select Import Source window, which allows you to select a device to import cardholder data from, such as a business card scanner

Select Host Wizard: Select Form

This form is used to select a cardholder record from those that matched the specified search criteria. The columns displayed are configured on the Cardholder Search Results form in the Cardholder Options folder. For more information, refer to Configure the Cardholder Search Results Lists on page 447.

This form is displayed when the [Next] button on the Select Host Wizard: Search form is clicked.



Cardholder listing window
A list of cardholder records that match the search criteria specified on the Select Host Wizard: Search form are displayed. The fields that are displayed in columns are set on the Cardholder Search Results Lists form in the Cardholder Options folder.

Back
Returns to the Select Host Wizard: Search form.

Finish

Completes the wizard. The selected cardholder's name will be displayed in the **Host name** field.

Cancel

Closes the window without selecting a cardholder and returns you to the Visit form in the Visits folder.

Help

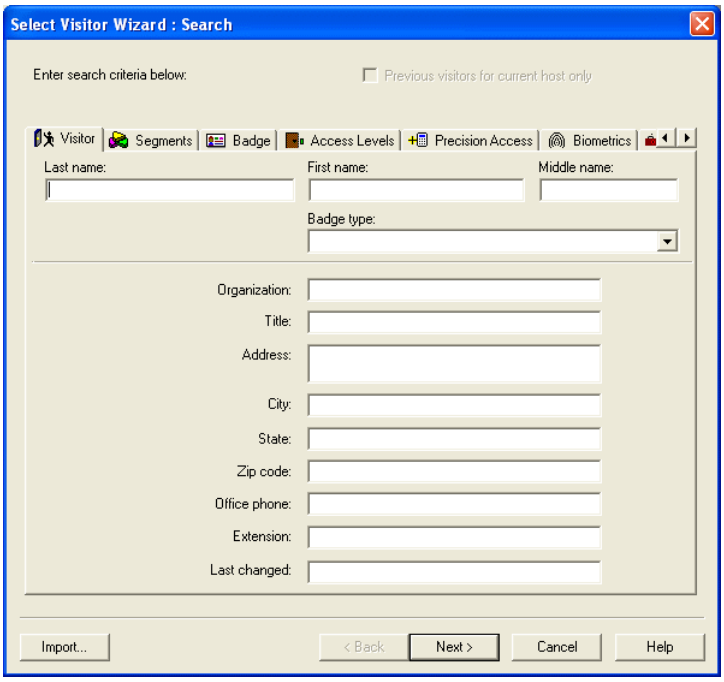
Displays online help for this topic

Select Visitor Wizard: Search Form

This form is used to locate visitor records that match the specified search criteria.

Note: If the FormsDesigner application has been used to customize your visitor data, the elements on your Select Visitor Wizard: Search form will be different. The default fields are pictured below.

This form is displayed when the [...] button to the right of the **Visitor name** drop-down list on the Visit form is clicked.



Previous visitors for current host only

This check box is only enabled when a cardholder has been selected and a visitor is being searched for. If selected, only those visitors who have previously visited the selected cardholder will be displayed on the Select Visitor: Select or Add form.

Last name

Indicates visitor's last name.

First name
Indicates visitor's first name.

Middle name
Indicates visitor's middle name.

Badge type
Indicates the visitor's badge type. Badge types are configured in the Badge Types folder. For more information, refer to Chapter 12: Badge Types Folder on page 307.

User-defined fields
All fields below the horizontal line on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.

Back
This button is not used.

Next
The wizard will proceed to the Select Visitor Wizard: Select or Add form.

Cancel
Closes the window without locating a visitor and returns you to the Visit form in the Visits folder.

Import
Displays the Select Import Source window, which allows you to select a device to import visitor data from, such as a business card scanner

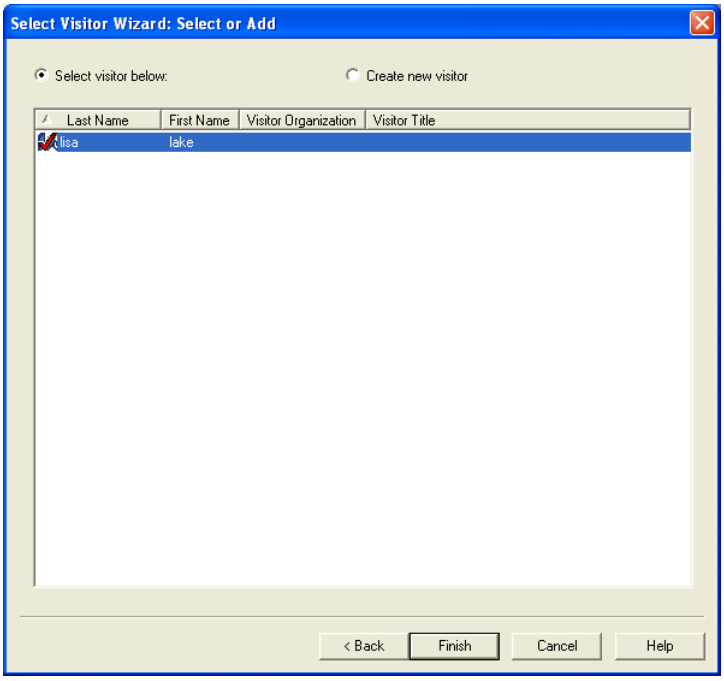
Help
Displays online help for this topic

Select Visitor Wizard: Select or Add Form

This form is displayed when adding a visit. From this form, you can:

- Search for visitor records that match the specified search criteria.
- Add a new visitor record.

This form is displayed when the [Next] button on the Select Visitor Wizard: Search form is clicked.



Select visitor below

Select this option if the visitor you need to add a visit for is listed below in the Visitor listing window. If you select this option, also select a visitor in the Visitor listing window below.

Create new visitor

Select this option if the visitor you need to add a visit for is not listed in the Visitor listing window.

If you select this option, the [Finish] button will be replaced with a [Next] button. When the [Next] button is clicked, the Select Visitor Wizard: Add form will be displayed, on which you can add a new visitor.

Visitor listing window

A list of visitor records that match the search criteria specified on the Select Visitor Wizard: Search form are displayed. The fields that are displayed in columns are set on the Visitor Search Results Lists form in the Cardholder Options folder.

Back

Returns to the Select Visitor Wizard: Search form.

Finish

This button is displayed only if **Select visitor below** is selected. Click this button to complete the wizard. The selected visitor's name will be displayed in the **Visitor name** field. If **Create new visitor** is selected, the [Finish] button is replaced by a [Next] button.

Cancel

Closes the window without selecting a visitor and returns you to the Visit form in the Visits folder.

Help

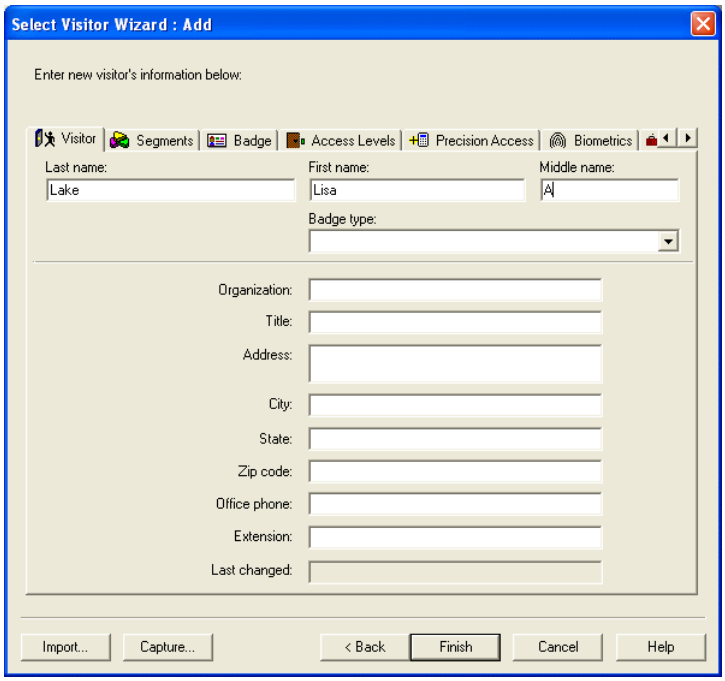
Displays online help for this topic

Select Visitor Wizard: Add Form

This form allows you to:

- Add a new visitor record
- Capture photographic information such as a photo, signature or biometric data for a visitor
- Import visitor data from a business card scanner or other similar device

This form is displayed when **Create new visitor** is selected and the [Next] button is clicked on the Select Visitor Wizard: Select or Add form.



Last name

Indicates visitor's last name.

First name

Indicates visitor's first name.

Middle name

Indicates visitor's middle name.

Badge type

Select the visitor's badge type. Badge types are configured in the Badge Types folder. For more information refer to Chapter 11: Badge Types Folder on page 243.

User-defined fields

All fields below the Name fields on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.

Import

Displays the Select Import Source window, which allows you to select a device to import visitor data from, such as a business card scanner

Capture
Displays Multimedia Capture, where you can capture photographic information such as a photo, signature or biometric data for a visitor

Back
Returns to the Select Visitor Wizard: Select or Add form.

Finish
Completes the wizard. The visitor record will be added to the database and the name of the visitor who was just added will be displayed in the **Visitor name** field.

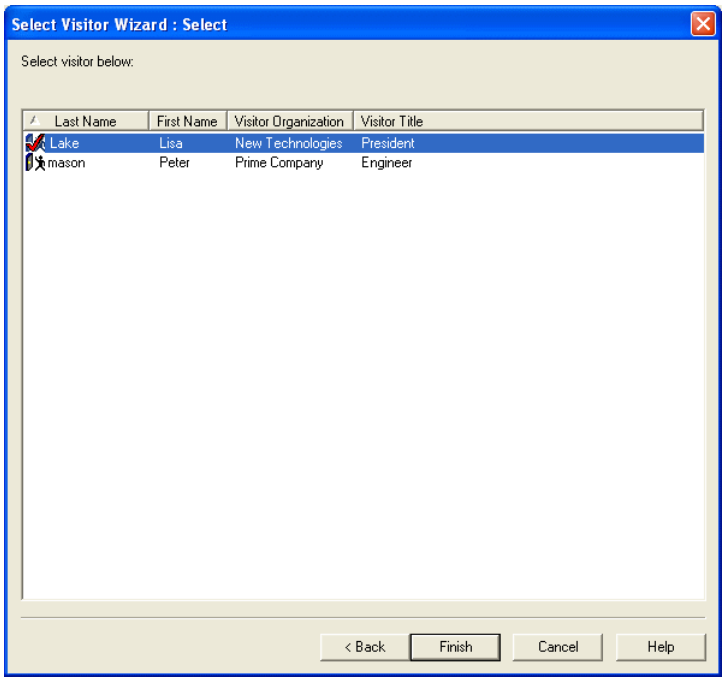
Cancel
Closes the window without adding a visitor and returns you to the Visit form in the Visits folder.

Help
Displays online help for this topic

Select Visitor Wizard: Select Form

This form is displayed when searching; it is used to select a visitor record from those that matched the specified search criteria.

This form is displayed when the [...] button to the right of the Visitor name field on the Visit form in the Visits folder is clicked.



Last Name
Indicates visitor's last name.

First Name
Indicates visitor's first name.

Middle Initial
Indicates visitor's middle initial.

User-defined fields
All fields below the Name fields on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.

Back
Returns to the previous form.

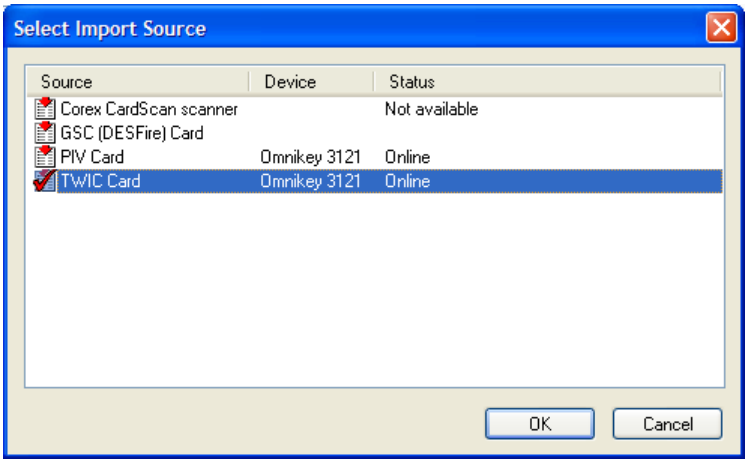
Finish
Completes the wizard. The selected visitor's name will be displayed in the **Visitor name** field.

Cancel
Closes the window without selecting a visitor and returns you to the Visit form in the Visits folder.

Help
Displays online help for this topic

Select Import Source Window

This window is displayed by clicking the [Import] button on any window in the Select Host Wizard or Select Visitor Wizard.



Source listing window
Displays a list of available sources, such as a business card scanner, to import cardholder or visitor data from.

OK
If a valid source is selected, you will be able to import cardholder or visitor data using it.

Cancel
Closes the Select Import Source window without selecting a source to import cardholder or visitor data from.

CHAPTER 6

Assets Folder

The Assets folder contains forms with which you can:

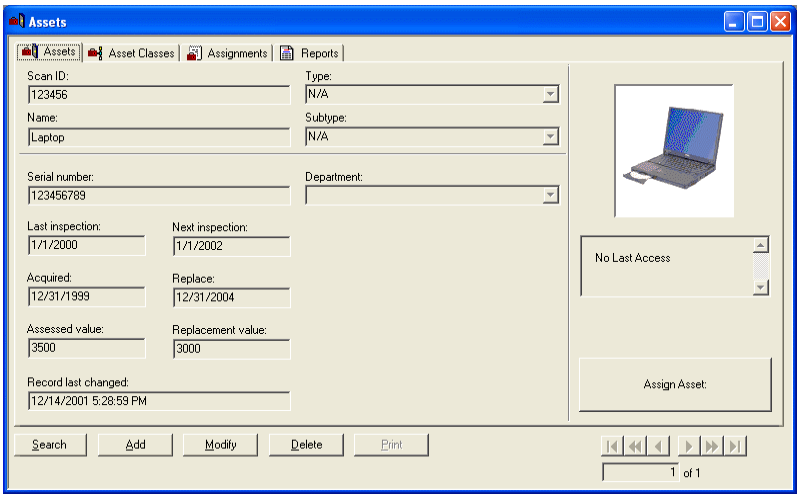
- Add, change or remove asset records.
- Assign assets to cardholders.
- Track assets that are assigned to cardholders.
- Preview and print asset reports.

The Assets folder contains four forms: the Assets form, the Asset Classes form, the Assignments form and the Reports form.

This folder is displayed by selecting ***Assets*** from the ***Administration*** menu, or by selecting the Assets button on the Administration toolbar.

Toolbar Shortcut

Assets Form



Scan ID

Enter the Scan ID of the asset.

Name

Enter a descriptive name for the asset. This is a “friendly” name assigned to each asset to make it easy to identify. Each name must be unique and contain no more than 32 characters.

Type

Select the type of asset being configured. Available choices depend on what asset types were added in the Asset Types and Subtypes Management window. The window is displayed by selecting ***Asset Types and Subtypes*** from the ***Asset*** menu.

Subtype

Select the subtype of the asset being configured. Available choices depend on what asset subtypes were added in the Asset Types and Subtypes Management window. The window is displayed by selecting ***Asset Types and Subtypes*** from the ***Asset*** menu.

Serial Number

Enter the serial number of the asset you are adding.

Department

Select the department of the asset being configured. Available choices depend on what departments were added in the List Builder folder.

Last Inspection

Enter the date when the asset was last inspected.

Next Inspection

Enter the date when the asset will be inspected next.

Acquired

Enter the date when the asset was acquired.

Replace
Enter the date when the asset will be replaced.

Assessed Value
Enter the assessed value of the asset.

Replacement Value
Enter the replacement value of the asset.

Record Last Changed
Indicates the date of when the selected asset record was last changed.

Photo
Displays a photo capture of the asset if one was added in Multimedia Capture.

Last Access
Displays the date and time of the asset's last access.

Assign Asset/Assign To
When adding or modifying an asset, select the [Assign Asset] button to launch the Cardholders folder. On the Cardholder form you can search for or add a cardholder to assign to the asset being configured.

Once you have located the cardholder on the Cardholder form, their name will appear on the [Assign To] push button. Click on this button to assign the asset to the cardholder.

If the Cardholders folder is already open and a cardholder record is displayed, then the [Assign To] button will automatically display the name of that cardholder record.

Search
Click on this button to search for an asset based on a value entered in one or more of the fields.

Last Search
Click on this button the display the findings of the previous search.

First
Moves to the first matching record.

Rewind
Moves 10 matching records back.

Previous
Moves to the previous matching record.

Next
Moves to the next matching record.

Fast Forward
Moves 10 matching records forward.

Last

Moves to the last matching record.

Record count

Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.

Add

Used to add an asset record.

Capture

Launches Multimedia Capture where you can add a photo of the asset.

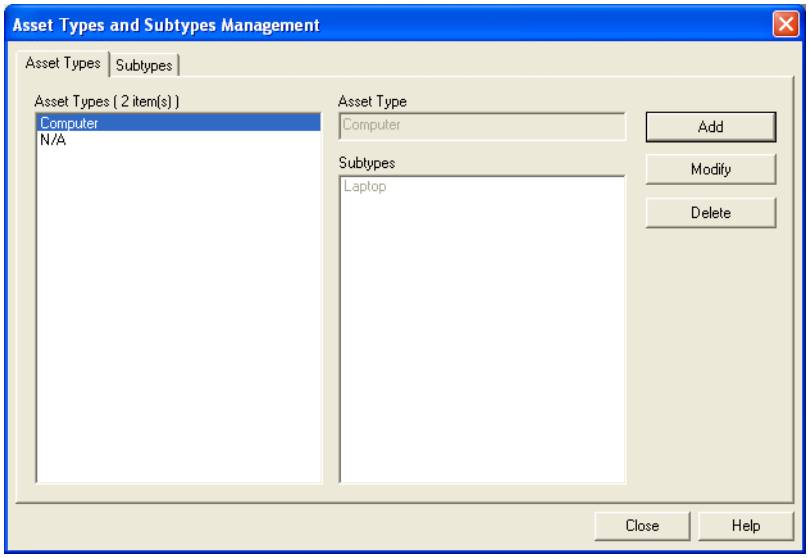
Modify

Used to change an asset record.

Delete

Used to delete an asset record.

Asset Types Form



Asset Types

Lists the names of all asset types that have been configured in the system.

Asset Type

In add or modify mode, specifies the name of the asset type.

Subtypes

Lists the subtypes that have been assigned the the selected asset type.

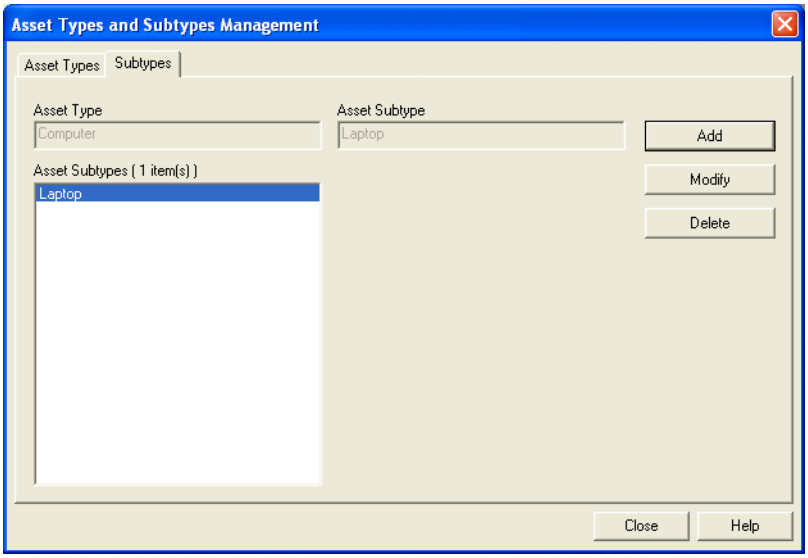
Add

Used to add an asset type.

Modify
Used to change an asset type.

Delete
Used to delete an asset type.

Subtypes Form



Asset Type
Displayed the name of the asset type that is selected on he Asset Type form.

Asset Subtype
In add or mosify mode, specifies the name of the subtype.

Asset Subtypes
Lists all asset subtypes that have been configured in the system.

Add
Used to add an asset subtype.

Modify
Used to change an asset subtype.

Delete
Used to delete an asset subtype.

Assets Form Procedures

The following procedures can be performed on this form.

Add an Asset

1. Select ***Assets*** from the ***Administration*** menu. The Assets folder opens.
2. Click [Add].
3. In the **Scan ID** field, enter an ID number for the asset.
4. In the **Name** field, enter a descriptive name for the asset. This is a “friendly” name assigned to each asset to make it easy to identify. Each name must be unique and contain no more than 32 characters.
5. If you want to identify the asset by type, select one from the **Type** drop-down list. If you want to identify the asset by subtype, select one from the **Subtype** drop-down list. If you don’t want to identify the asset by type and/or subtype, choose N/A from the **Type** and **Subtype** drop-down lists.
6. Type in a **Serial Number** and then choose the **Department** of the asset from the drop-down list.
7. Enter the date of the asset’s **Last Inspection** and the date of the asset’s **Next Inspection**.
8. Enter the date of when the asset was acquired in the **Acquired** field.
9. Enter the date of when the asset will be replaced in the **Replace** field.
10. In the **Assessed Value** field type the amount, in dollars, of the asset’s value. In the **Replacement Value** field type the amount, in dollars, it will cost to replace the asset.
11. Click [Capture] to launch Multimedia Capture from where you can capture a photo of the asset to be displayed on the Assets form. For more information please refer to Appendix C: Multimedia Capture on page 1339.
12. You can switch to the Asset Classes form if you want to configure groups and classes now. For more information, refer to Asset Classes Form Procedures on page 186.
13. Click [OK].

Modify an Asset

1. Locate the asset record that you want to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save your changes, or [Cancel] to revert to the previously saved values.

Delete an Asset

1. Locate the asset record that you want to delete.
2. Click [Delete].
3. Click [OK].

Assign a Cardholder to an Asset

1. Locate the asset record that you want to assign.
2. If the Cardholders folder was already open and a cardholder record displayed, proceed to 3. If not, click [Assign Asset] to launch the Cardholders folder.
3. In the Cardholders folder, retrieve the record of the cardholder you want to assign to the asset. On the Assets form of the Assets folder, the name of the cardholder will appear in the [Assign To] push button.
4. Click [Assign To] to assign the asset.

Search for an Asset Record

1. Select ***Assets*** from the ***Administration*** menu. The Assets folder opens.
2. Click [Search].
3. Specify your search criteria by typing full partial entries in the enabled fields.
4. Click [OK].

   OnGuard retrieves and displays the first matching record. Use the , , , , and buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

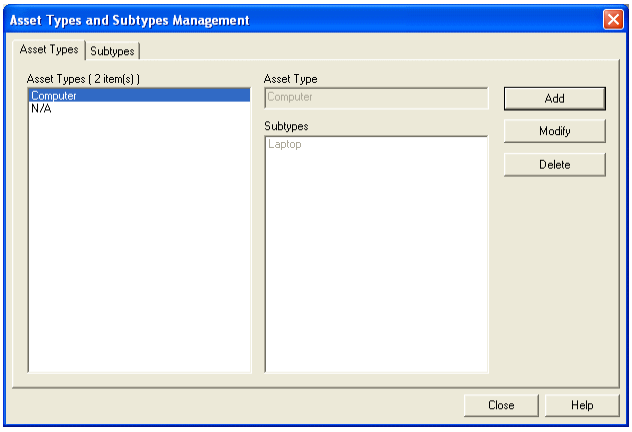
Retrieve the Most Recent Search Results

1. Click [Search].
2. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
3. If you want, modify your search criteria.
4. Click [OK].

OnGuard retrieves and displays the first matching record. Use the , , , , and buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

Add an Asset Type/Subtype

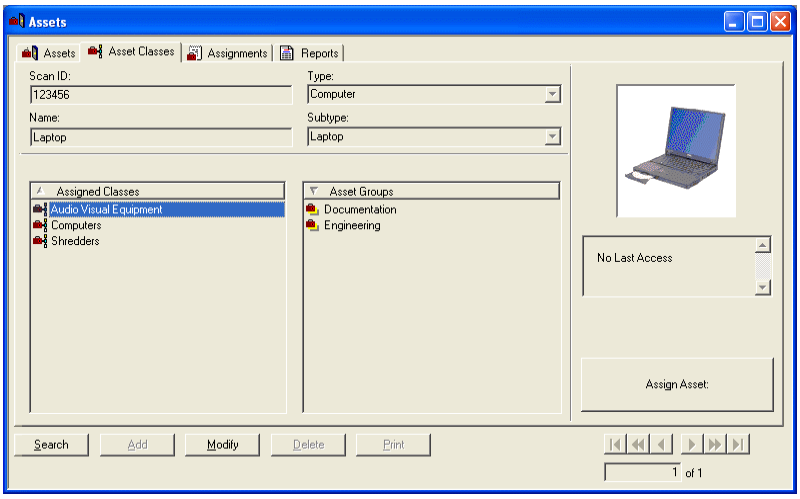
1. Select ***Assets*** from the ***Administration*** menu. The Assets folder opens.
2. Select ***Asset Types and Subtypes*** from the ***Asset*** menu. The Asset Types and Subtypes Management window opens.



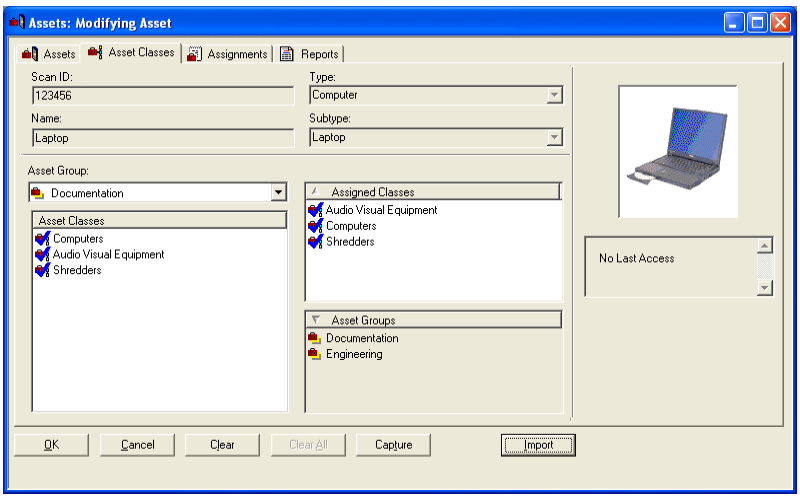
3. Select and asset type in the Asset Types listing window. If you want to modify a subtype, select the Subtype tab first.
4. Click [Modify] and make your desired changes.
5. Click [OK].
6. Click [Close] to return to the Assets form.

Asset Classes Form

Asset Classes Form (View Mode)



Asset Classes Form (Modify Mode)



Scan ID

Indicates the Scan ID of the asset.

Name

Indicates the name of the asset.

Type

Indicates the type of asset being configured.

Subtype

Indicates the subtype of the asset being configured.

Assigned Classes

(View and modify mode) Displays the classes that are currently assigned to a group in the Asset Groups listing window.

Asset Groups
(View mode) Displays the asset groups that correspond with the classes in the Assigned Classes listing window.

Asset Group
(Modify mode) Select the asset group(s) to which the asset will belong.

Asset Classes
Select the asset classes that will be assigned to the asset. Groups can contain as many as 32 classes, but each asset can only belong to as many as 15 classes.

Photo
Displays a photo capture of the asset if one was added in Multimedia Capture.

Last Access
Displays the date and time of the asset's last access.

Assign Asset/Assign To
When adding or modifying an asset, select the [Assign Asset] button to launch the Cardholders folder. On the Cardholders form you can search for or add a cardholder to assign to the asset being configured.

Once you have located the cardholder on the Cardholders form, their name will appear on the [Assign To] push button. Click on this button to assign the asset to the cardholder.

If the Cardholders folder is already open and a cardholder record is displayed, then the [Assign To] button will automatically display the name of that cardholder record.

Search
Click on this button to search for an asset based on a value entered in one or more of the fields.

Last Search
Click on this button the display the findings of the previous search.

First
Moves to the first matching record.

Rewind
Moves 10 matching records back.

Previous
Moves to the previous matching record.

Next
Moves to the next matching record.

Fast Forward
Moves 10 matching records forward.

Last

Moves to the last matching record.

Record count

Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.

Add

This button is not used.

Modify

Used to change an asset classes record.

Delete

This button is not used.

Print

This button is not used.

Asset Classes Form Procedures

The following procedures can be performed on this form.

Assign Classes to an Asset

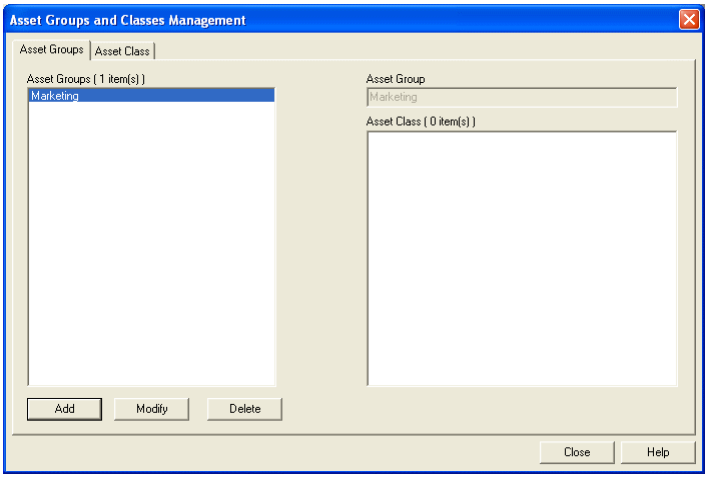
1. Locate the record of the asset that you want to assign classes to.
2. Click [Modify].
3. Select an **Asset Group** from the drop-down list.
4. In the Asset Classes listing window, select the classes you want to assign. You can select as many as 15 classes for each asset.
5. Click [OK].

Modify an Asset Classes Assignment

1. Locate the record of the asset that you want to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save your changes, or [Cancel] to revert to the previously saved values.

Add Asset Groups and Classes

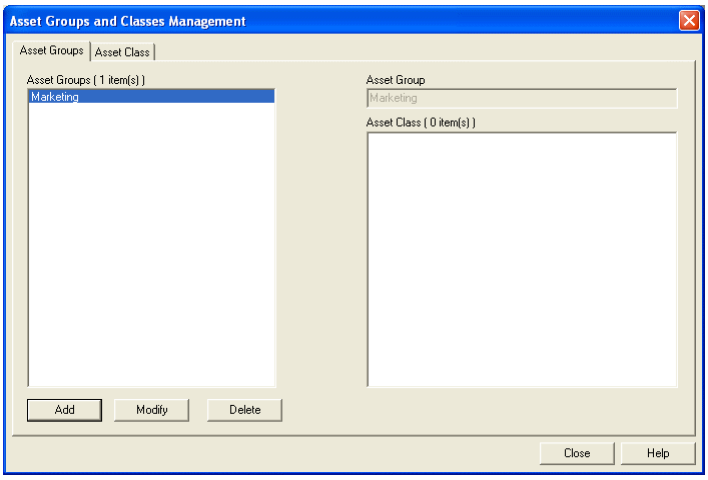
1. Select ***Assets*** from the ***Administration*** menu.The Assets folder opens.
2. Select ***Asset Groups and Classes*** from the ***Asset*** menu. The Asset Groups and Classes Management window opens.



3. To add an asset group:
   a. Click the Asset Groups tab.
   b. Click [Add].
   c. In the **Asset Group** field, enter the name of the group you are adding.
   d. Click [OK].
4. To add an asset class:
   a. Click the Asset Class tab.
   b. Click [Add].
   c. In the **Asset Class** field, enter the name of the class you are adding. You can add as many classes as you want but you can only assign as many as 32 classes to a group.
   d. Click [OK].
5. To assign a class to a group:
   a. Click the Asset Class tab.
   b. Select an asset class.
   c. Click [Modify].
   d. Select the name of an asset group.
   e. Click the <-- push button to remove the asset group. Click the --> push button add the asset group.
   f. Click [OK].

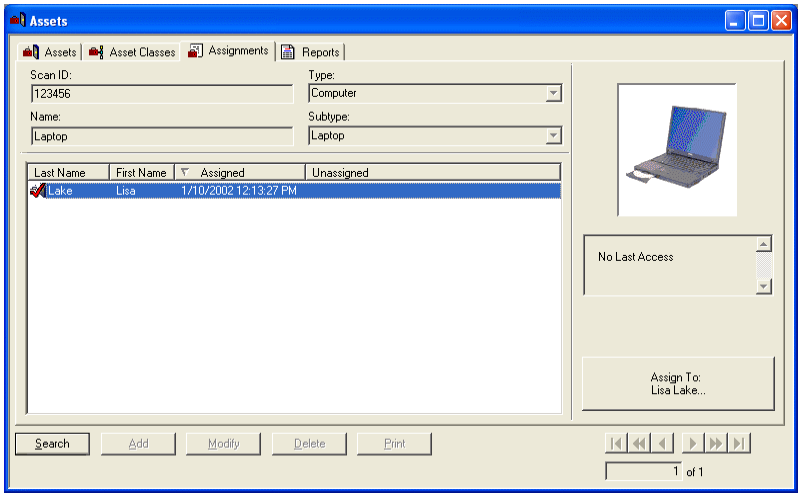
Modify Asset Groups and Classes

1. Select ***Assets*** from the ***Administration*** menu.The Assets folder opens.
2. Select ***Asset Groups and Classes*** from the ***Asset*** menu. The Asset Groups and Classes Management window opens.



3. To modify asset classes within a group:
   a. Click the Asset Groups tab.
   b. Select the name of a group
   c. Click [Modify].
   d. Select the name of the class you want to add or remove.
   e. Click the <-- push button to remove the asset class from the group. Click the --> push button to add the asset class to the group.
   f. Click [OK].
4. To modify the asset groups an asset class is assigned to:
   a. Click the Asset Class tab.
   b. Select the name of the asset class.
   c. Click [Modify].
   d. Select the name of the asset group you want to add or remove.
   e. Click the <-- push button to remove the asset group. Click the --> push button add the asset group.
   f. Click [OK].

Assignments Form



Scan ID

Displays the assets scan ID. If you click [Search], you can enter the scan ID you want to search.

Name

Displays the name of the asset. If you click [Search], you can enter the name of the asset you want to search.

Type

Displays the type of asset. If you click [Search], you can enter the type of asset you want to search.

Subtype

Displays the subtype of the asset. If you click [Search], you can enter the subtype of the asset you want to search.

Listing window

Displays a list of cardholders who are currently or have been assigned to the selected asset.

You can choose the number of entries you want listed by selecting ***Show Assignments X Days Past*** from the ***Asset*** menu.

Last Name

When you select the [Search] button, enter the last name of a cardholder to locate the assets that have been assigned to them.

First Name

When you select the [Search] button, enter the first name of a cardholder to locate the assets that have been assigned to them.

Assigned

When you select the [Search] button, enter the date the asset was assigned if you want to locate the cardholder who was assigned to the asset on that date.

Unassigned

When you select the [Search] button, enter the date the asset was unassigned if you want to locate the cardholder who was unassigned to the asset on that date.

Photo
Displays a photo of the asset if one was captured in Multimedia Capture.

Last Access
Displays the date and time of the assets last access.

Assign Asset/Assign To
Displays the name of the asset currently displayed in the Cardholders folder. If no name is displayed, when selected the Cardholders folder is launched from where you can search for and select the cardholder you wish to assign to the asset.

Search
Used to locate a cardholder or asset assignment record.

Last Search
Click on this button the display the findings of the previous search.

First
Moves to the first matching record.

Back 10
Moves 10 matching records back.

Previous
Moves to the previous matching record.

Next
Moves to the next matching record.

Forward 10
Moves 10 matching records forward.

Last
Moves to the last matching record.

Record count
Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.

Assignments Form Procedures

The following procedures can be performed on this form.

Assign a Cardholder to an Asset

1. Locate the record of that asset that you want to assign.
2. If the Cardholders folder was already open and a cardholder record displayed, proceed to 3. If not, click [Assign Asset] to launch the Cardholders folder.
3. On the Cardholders folder, retrieve the record of the cardholder you want to assign to the asset. On the Assignments form of the Assets folder, the name of the cardholder will appear in the [Assign To] push button.
4. Click [Assign To] to assign the selected asset to the selected cardholder. The name of the cardholder will appear in the listing window.

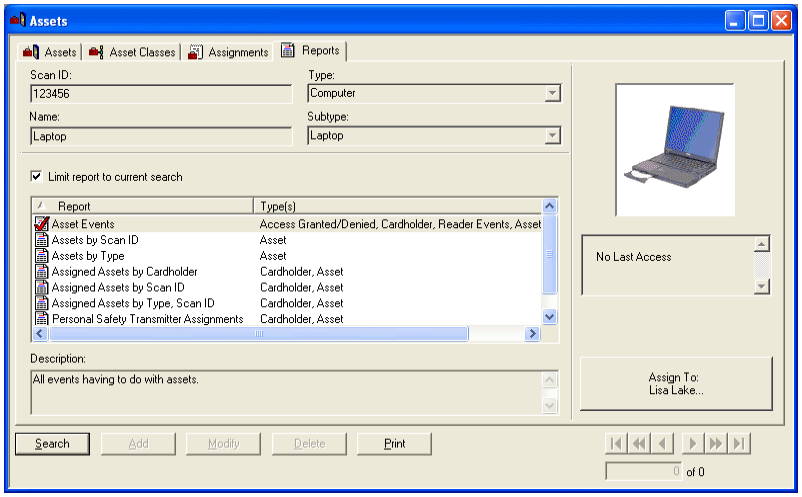
Unassign an Asset

1. Locate the record of the asset that you want to unassign.
2. In the listing window, select the name of the cardholder who is currently assigned to the asset. The entry of the cardholder who is assigned will not list an **Unassigned** Date.
3. Right-click on the cardholder entry you selected and choose ***Unassign Asset*** from the menu. The **Unassigned** field will be updated to the current date.

Search for a Cardholder Assigned to an Asset

1. Locate the asset record that you want to look up a cardholder for.
2. In the listing window, select the name of the cardholder you want to look up.
3. Right-click on the cardholder entry you selected and choose ***Find Cardholder*** from the menu. The Cardholders folder will display the record of the cardholder you selected.

Reports Form



Scan ID

Displays the scan ID of the selected asset.

Name
Displays the name of the selected asset.

Type
Displays the type of the selected asset.

Subtype
Displays the subtype of the selected asset.

Listing window

Displays a list of the types of reports that can be previewed and/or printed. An icon precedes each entry.

Limit report to current search
Select this check box if you want to limit this report to the search that you just completed.

Description
Displays a description of the report type you selected from the listing window.

Filename
Displays the file name of the report type.

Photo
Displays the captured photo of the currently selected asset.

Last Access
Displays the date and time of the asset's last access.

Assign Asset/Assign To
Displays the name of the cardholder currently displayed in the Cardholders folder. If no name is displayed, when selected the Cardholders folder is launched from where you can search for and select the cardholder you wish to assign to the selected asset.

Print
This button launches the Report Print Options window from where you can preview, print or export a report.

First

Moves to the first matching record.

Back 10

Moves 10 matching records back.

Previous

Moves to the previous matching record.

Next

Moves to the next matching record.

Forward 10

Moves 10 matching records forward.

Last

Moves to the last matching record.

Record count

Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10.

You can type in a number and hit the <Enter> key to jump to that record number.

Close

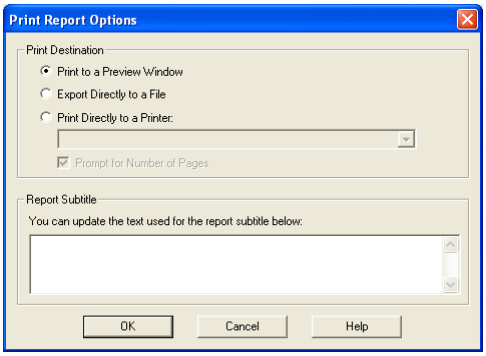
Closes the Assets folder.

Reports Form Procedures

The following procedures can be performed on this form.

Run an Asset Report

1. In the listing window, select the type of report you want to run.
2. Select the **Limit report to current search** check box if you want to limit this report to the search that you just completed.
3. Click [Print]. The Print Report Options window will be displayed.



4. Choose a Print Destination and if you want, update the text used for the report subtitle.
5. Click [OK].
   - If you chose the **Print Directly to a Printer** radio button, select a printer from the drop-down list. If you select the **Prompt for Number of Pages** check box, the Print window will be displayed where you can select print range, number of copies and whether or not to collate your report.
   - If you chose the **Export Directly to a File** radio button, the Export window will be displayed. Choose the report Format and Destination from the drop-down lists. Depending on what you chose, enter the destination and format information in the corresponding window, then click [OK].

- If you chose the **Print to a Preview Window** radio button, an asset report print preview window will be displayed from where you can view the selected report on the screen. For more information, refer to Chapter 10: Report Print Preview Window on page 241.

CHAPTER 7

Badge Templates Folder

IMPORTANT: To view the Badge Templates folder your system must have an ILS license.

The Badge Templates folder is used to configure badge templates that can be downloaded to an ILS lock and assigned to a single cardholder. Badge templates are ideally used in dynamic environments where cardholders change frequently. Badge templates can be used to avoid numerous data downloads to the locks that are in such a dynamic environment.

Badge templates allow you to set up pre-defined access to locks as well as the ability to control and monitor the access of the cardholders assigned to the badge templates. Since only one cardholder can be assigned to a badge template at a time, each new card that is issued to a badge template will lock out the previous card made from that badge template.

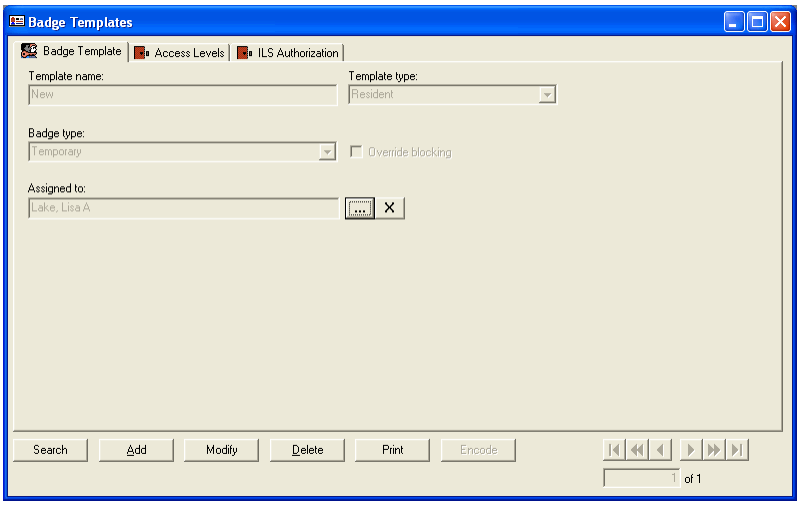
For more information please refer to Appendix K: Lenel ILS (Integrated Locking Solutions) on page 1473.

Note: In order to configure badge templates on an Enterprise Regional Server or a Mobile Station you must first add at least one badge template to the Enterprise Master or Distributed ID server. Once complete you must then run Replicator and perform a cardholder download from the master server to the regions.

IMPORTANT: ILS readers (locks) do not support assigning an access level to a cardholder (badge) if that access level contains a lock that is in an access level already assigned to the cardholder (badge).

Badge Template Form

The Badge Template form is used to configure the template name and type and to assign the template to a cardholder.



Template name

Used to create a name for the template.

Template type

Select the template type. Your choices are:

- **Resident** - Use for long term cardholders
- **Visitor** - Use for short term cardholders

Badge type

Select the cardholder's badge type. Only a badge type that uses an automatic ID allocation type can be selected for a badge template. Badge types are configured in the Badge Types folder. For more information, refer to Chapter 12: Badge Types Folder on page 307.

Override blocking

Select this to give the cardholder assigned to this badge template the ability to unlock a door that has been blocked with a blocking card. Locks are blocked to deny entrance in unusual cases such as a police investigation. It is important to leave this field unselected unless you are certain the user of this badge template should be able to open a blocked lock. For more information, refer to Configure Blocking Cards for Integra Locks on page 1488 or Configure Special Purpose Cards for ILS Offline/Wireless Locks on page 1511.

Assigned to

Click the [...] button to open the Select Cardholder Wizard to search for or create a cardholder. Click the [X] button to unassign the cardholder from the badge template. You can also type in the name of the cardholder in the Assigned to text box to search for a specific cardholder.

Search all assigned

Only available in search mode. Select to only search for badge templates that have a cardholder assigned.

Search all unassigned

Only available in search mode. Select to only search for badge templates that do not have a cardholder assigned.

Search
Click this button to search all assigned or unassigned badge templates, and then use the Badge Template Assignment Wizard to search for an existing cardholder or to create a new cardholder.

Add
Used to add a badge template.

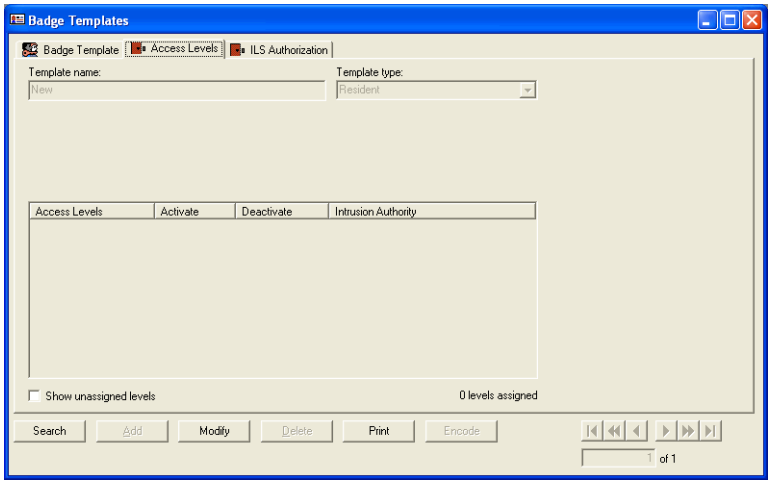
Modify
Used to change a badge template.

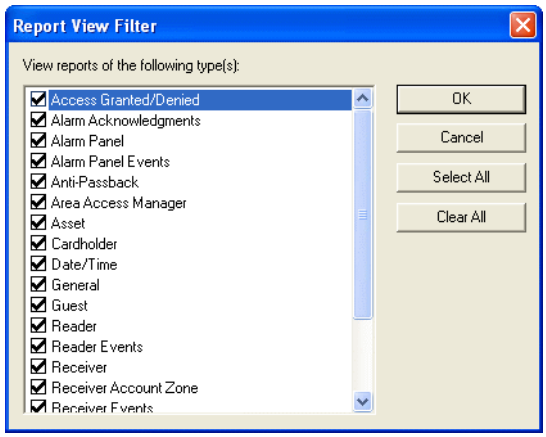
Delete
Used to remove a badge template.

Print
Opens the Badge Printing window.

Access Levels Form

The Access Levels form is used to assign access levels to the badge templates.





Intrusion Authority

The authority levels assigned act as access levels. Make note of this as the maximum number of access levels is usually 32.

Displayed in modify mode. When selected, displays the Intrusion Authority Levels form from where you can assign intrusion authority levels. These levels will allow the cardholder the ability to issue commands via the keypad. For more information, refer to Chapter 34: Command Keypad Templates Folder on page 743.

The intrusion authority functionality is only used by Lenel online access control hardware and not offline locking systems.

Activate Dates

Displayed in modify mode. When selected, displays the Access Level Activation Dates form from where you can select the dates when the selected access level will become valid and invalid.

Access Groups

Displayed in modify mode. When selected, displays the Select Access Levels in a Group form from where you can choose the access level group that you want to select access levels from.

Access Levels listing window

Lists the access levels that can be added to the badge template.

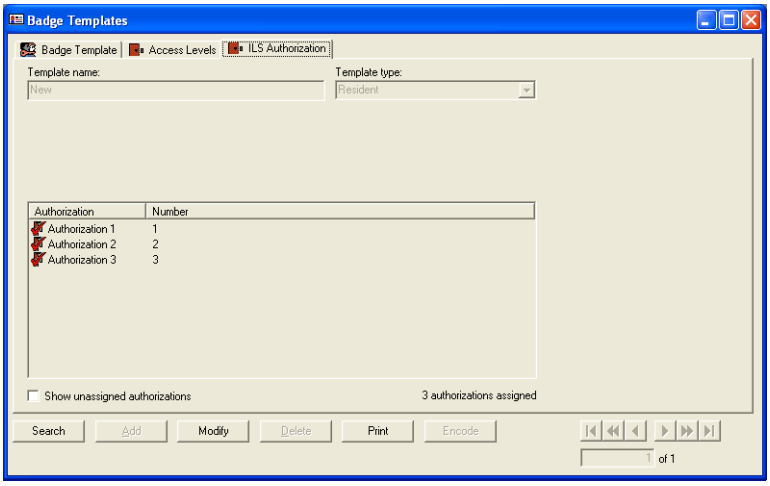
Show unassigned levels

Displayed in view and modify mode. When selected, the **Access levels** display lists both access levels that have been and that can be assigned to the selected cardholder/badge record.

ILS Authorization Form

The ILS Authorization form is used to add authorization levels to the badge templates.

Note: To view this form your system must have an ILS license.



Authorization listing window

Lists the ILS authorizations that can be assigned to the badge template.

Assign All

Displayed in modify mode. Click to assign all authorizations displayed in the authorization listing window.

Unassign All

Displayed in modify mode. Click to unassign all authorizations displayed in the authorization listing window.

Show unassigned authorizations

Displayed in view mode. When selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected badge template.

Badge Template Form Procedures

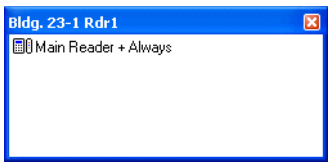
Use the following procedures for this form.

Add a Badge Template

1. Select ***Badge Templates*** from the ***Administration*** menu. The Badge Templates folder opens.
2. On the Badge Template tab click [Add].
3. Enter a template name in the Template name field.
4. Select a template type from the **Template type** drop-down box.
5. Select a badge type from the **Badge type** drop-down box.
6. Optionally, you can select the **Override blocking** check box.
7. In view mode, on the **Assigned to** field, click the [...] button to start the Select Cardholder Wizard. The wizard will allow to you to create or search for a specific cardholder that you wish to assign the badge template to. Click [OK].

   For more information, refer to Assign a Cardholder to a Badge Template on page 200.
8. Select the Access Levels tab and click [Modify].
9. Select the **Show unassigned levels** check box. The **Access levels** display will list both access levels that have been and that can be assigned to the selected cardholder/badge record.

Note: To find out more about a particular access level, either double-click on an access level entry, or right-click on an access level entry and select **Level Definition**. A popup window opens, listing the reader/time zone combinations that define the access level. For example:



10. Optional: If you would like to set the date and time that the badge will deactivate:
    a. Click [Activate Dates]. The Access Level Activation Dates window opens.
    b. Deselect the [Activation Date] radio button.
    c. Select the [Deactivation Date] radio button and select the date and time that the access level should deactivate.

d. Click [OK].

11. Optional: If you want to assign all the access levels that belong to an access group:
    a. Click [Access Groups]. The Select Access Levels in a Group window opens.
    b. The Select Access Levels in a Group window lists all currently defined access groups. You can expand an entry to display the list of access levels that make up a group. Select an access level or an access group. If you select an access group, you select all of the access levels it contains.
    c. Click [Select].
    d. Click [Yes].
12. Select the ILS Authorization tab.
13. In the authorization listing window select the authorizations that you want the cardholder to have. For more information, refer to ILS Authorization Form on page 136.
14. Click [OK]. The cardholder now has access to the authorization levels you have selected.
15. The badge template is now created.

Assign a Cardholder to a Badge Template

1. Create a new badge template or search for an unassigned badge template.
2. Select ***Badge Templates*** from the ***Administration*** menu. The Badge Templates folder opens.
3. On the Badge Template tab, search for the template you would like to add a cardholder to and click [Modify].
4. On the **Assigned to** field click the browse button. The Badge Template Assignment Wizard window opens.
5. Select whether you would like to search for an existing cardholder or create a new cardholder. If you choose to create a new cardholder then fill in all appropriate information and click [Finish]. The cardholder will automatically be added to the badge template and the wizard will finish.
6. If you are searching for a cardholder, fill in as much information as you can and click [Next]. A list of cardholders matching your search criteria will be listed.
7. Select the cardholder you wish to add and click [Next].
8. Review and configure any settings for the selected cardholder. Click [Finish].
9. If you wish to assign a personalized access level assignment, Select the Access levels tab and select an access level in the listing window. Assigning an access level to a cardholder in the badge template will create a personalized access level that can be seen in the Assignment Type column of the Access Levels listing window.

Unassign a Cardholder from a Badge Template

1. Select ***Badge Templates*** from the ***Administration*** menu. The Badge Templates folder opens.
2. On the Badge Template tab, search for the template you would like to unassign cardholders from.
3. On the **Assigned to** field click [X] to unassign the cardholder. Unassigning the cardholder also removes any personalized access level assignments.

Move a Cardholder to a Different Badge Template

1. Select ***Badge Templates*** from the ***Administration*** menu. The Badge Templates folder opens.
2. On the Badge Template tab, search for the template whose cardholder you would like to move to a different badge template.
3. On the **Assigned to** field, click [...].

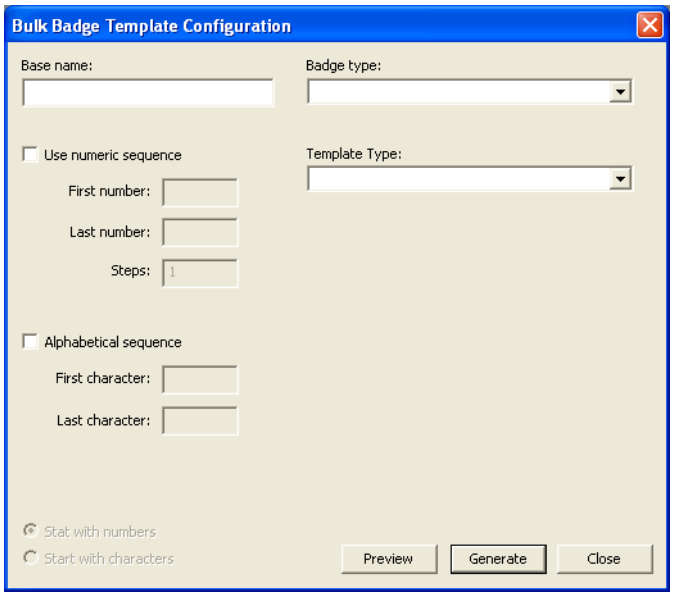
4. The Select Badge Template Operation dialog opens. Select the **Move cardholder to another badge template** radio button. The Badge Template Move Wizard window opens.
5. In the Badge Template Move Wizard window, enter the search criteria for the template you would like to move the cardholder to and click [Next].
6. A list of matching templates are listed. Select which one you would like to move the cardholder to. Click [Finish]. The cardholder and any personalized access level assignments that were assigned to that cardholder are now moved to the new badge template.

Issue a New Badge to an Existing Cardholder

1. Select ***Badge Templates*** from the ***Administration*** menu. The Badge Templates folder opens.
2. On the Badge Template tab, search for the template whose assigned cardholder information you would like to update before issuing the new badge.
3. On the **Assigned to** field click [...].
4. The Select Badge Template Operation dialog opens. Select the **Issue a new badge for this cardholder** radio button. The Badge Template Issue New Badge window opens.
5. In the Badge Template Issue New Badge window, review and configure the settings for the badge template. Click [Finish].

Bulk Badge Template Configuration Form

The Bulk Badge Template Configuration form is used to add up to 2000 badge templates at once.



Base name

Enter the name that will appear for each badge template you are creating.

Use numeric sequence

Select to amend the base name with a number. You can further select the number that will start the sequence, end the sequence, and by what multiplier the sequence will use.

Alphabetical sequence

Select to amend the base name with a letter. You can further select what letters will start and end the sequence.

Start with numbers

If you are using the numeric sequence option select the **Start with number** radio button to add the numbers to the beginning of the base name.

Start with Characters

If you are using the alphabetical sequence option select the **Start with characters** radio button to add the letters to the beginning of the base name.

Badge type

Indicates the cardholder's badge type. Badge types are configured in the Badge Types folder. For more information, refer to Chapter 12: Badge Types Folder on page 307.

Template type

Select the template type. Your choices are:

- **Resident** - Use for long term cardholders
- **Visitor** - Use for short term cardholders

Preview

Click to preview the badge templates you are going to create.

Generate

Click to begin the process of creating the badge templates.

Add Bulk Badge Templates

Note: You can create up to 2000 badge templates for each bulk add.

1. Select ***Badge Templates*** from the ***Administration*** menu. The Badge Templates folder opens. A Badge Template menu item appears.
2. Select ***Badge Template > Bulk > Add Templates***. The Bulk Badge Template Configuration opens.
3. Enter a base name in the **Base name** field. This is the name each template in the bulk add will begin with.
4. Select whether you want the sequence of templates added to be numeric or alphabetical. This adds either numbers or letters to the base name of your template.
5. Select either the **Start with numbers** or **Start with characters** radio button.
6. In the **Badge type** field, select the badge type you want each template to use.
7. In the **Template type** field, select the template type you want each template to use.
8. To preview the names of the badge templates that will be bulk added click [Preview].
9. To start the bulk badge templates click [Generate] and follow the on screen instructions.

Bulk Unassign Cardholders from Badge Templates

1. Select ***Badge Templates*** from the ***Administration*** menu. The Badge Templates folder opens.
2. Search for the badge template(s) that you wish to remove cardholder(s) from.
3. Select ***Badge Template > Bulk > Unassign Cardholders in Search***.

4. You will be prompted as to whether you want to continue with the operation of removing the cardholders from the badge template. Click [OK] to continue with the process.

Badge Template Assignment Wizard

The Badge Templates Assignment Wizard allows you to search or assign cardholders to the badge template. For information on the specific fields, refer to Cardholder Form on page 98.

Badge Template Issue New Badge Wizard

The Badge Templates Issue New Badge window allows you to issue a new badge to an existing cardholder assigned to a badge template. For information on the specific fields, refer to Badge Template Form on page 195.

Badge Template Move Wizard

The Badge Templates Move Wizard allows you to move an existing cardholder to another badge template. For information on the specific fields, refer Badge Template Form on page 195.

CHAPTER 8

Reports Folder

The Reports folder contains forms with which you can:

- View on the screen reports created using report layout templates in the database and current data
- Report on data that meets specified criteria (such as dates, times, readers, alarm panels, cardholders and badge IDs)
- Print a report, save it to a file or export the data

The folder contains eight forms: the Report Configuration form, the Reader Reports form, the Alarm Panel Reports form, the Anti-Passback Reports form, the Date/Time Reports form, the Event Reports form, the Receiver Account Zone Reports form, and the Alarm Acknowledgment Reports form.

This folder is displayed by selecting ***Reports*** from the ***Administration*** menu or by selecting the Reports toolbar button.

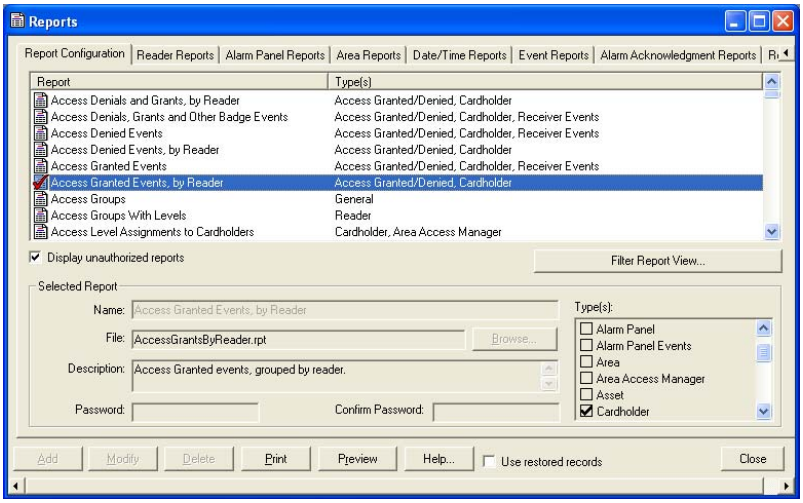
Toolbar Shortcut

Reports are installed when Database Setup is run. All reports are installed on the database server in the **ReportTemplates** subdirectory on the OnGuard installation disc. By default, this location is **C:\Program Files\OnGuard\ReportTemplates**.

Note: Refer to the release notes for the versions of Seagate Crystal Reports that are supported. The release notes are located in the **C:\Program Files\OnGuard\doc\en-US** subdirectory on the OnGuard installation disc.

For more information please refer to Appendix D: Reports on page 1401.

Report Configuration Form



Listing window

Lists currently defined reports of the type(s) selected in the Report View Filter window that the user is authorized to preview. Note that some reports are categorized under more than one type.

Display unauthorized reports

By default, the reports forms only list reports that users have permissions to preview. If the **Display unauthorized reports** check box is selected, reports that are disabled for a user will appear in the Report Configuration Form listing window. The user can identify which reports are disabled by whether the [Print] and [Preview] buttons are inactive. This allows the user to ask the system administrator for permission to an existing report, if desired.

Reports are authorized and unauthorized by using report permission groups. For more information, refer to Report Permission Groups Form on page 371.

Filter Report View

Click this button to display the Report View Filter window from where you can choose the types of reports you wish to view.

Name

The name of the report.

File

The location and name of the file that contains the report.

Browse

Used to search through drives and directories to choose a report filename to insert into the **File** field.

Description

A brief description of the report contents.

Password

This field is optional. If you type a password here, a user attempting to print this report will be asked to first enter the correct password. A password can be from 1 to 32 characters in length. As you type, the password will appear in the field as a series of *s.

Confirm Password
If you typed something in the **Password** field, you must type exactly the same thing here. As with the **Password** field, your entry here will appear as a series of *s.

Type(s)
Lists the types of reports that you can configure. The system reports that are included with the installation are each assigned an appropriate Type. You can modify report types on the system reports but selecting invalid types could result in unwanted behavior.

To restore types back to their defaults, run Database Setup.

To make the report appear in Area Access Manager the Area Access Manager check box must be selected in the Types field.

Add
Used to configure a report.

Modify
Used to change a report configuration.

Delete
Used to remove a report.

Print
Opens the Print Report Options window.

Preview
Displays the selected report in the Report Print Preview window.

Help
Displays relevant on-screen help for this form.

Use restored records
If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions.

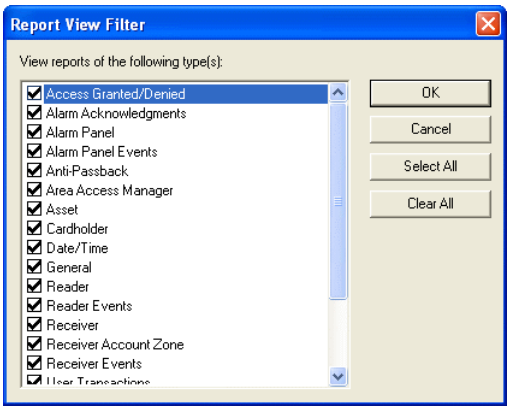
Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information, refer to Chapter 23: Archives Folder on page 501.

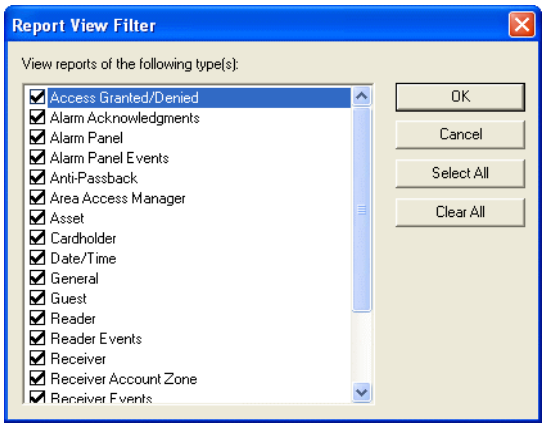
Mode
In view mode, indicates the number of reports selected in the listing window and the total number of reports contained in all selected categories. For example: “1 of 42 selected.” In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the Reports folder.

Report View Filter Window

This window is displayed by clicking the [Filter Report View] button on the Report Configuration form.





Access Granted/Denied

If this check box is selected, Access Granted and Access Denied reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.

Alarm Acknowledgments

If this check box is selected, Alarm Acknowledgment reports will be included in the listing window.

Alarm Panel

If this check box is selected, Alarm Panel reports will be included in the listing window. Reports of this type appear on the Alarm Panel Reports form for filtering.

Alarm Panel Events

If this check box is selected, Alarm Panel Events reports will be included in the listing window. Reports of this type appear on the Alarm Panel Reports form for filtering.

Anti-Passback

If this check box is selected, Anti-Passback reports will be included in the listing window. Reports of this type appear on the Anti-Passback Reports form for filtering.

Asset

If this check box is selected, Asset reports will be included in the listing window. Reports of this type appear on the Asset Reports form for filtering.

Cardholder
If this check box is selected, Cardholder reports will be included in the listing window. Reports of this type appear on the Reports form of the Cardholder folder for filtering.

Date/Time
If this check box is selected, Date/Time reports will be included in the listing window. Reports of this type appear on the Date/Time Report form for filtering.

General
If this check box is selected, general reports will be included in the listing window.

Reader
If this check box is selected, Reader reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.

Reader Events
If this check box is selected, Reader Events reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.

Receiver
If this check box is selected, the names of Receiver reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.

Receiver Account Zone
If this check box is selected, the names of Account Zone reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.

Receiver Events
If this check box is selected, the names of Receiver Events reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.

User Transactions
If this check box is selected, User Transactions reports will be included in the listing window. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder.

Video Events
If this check box is selected, Video events reports will be included in the listing window.

Visitor
If this check box is selected, Visitor reports will be included in the listing window.

OK
Click this button to save your changes and return to the Report Configuration form.

Cancel
Click this button to return to the Report Configuration form without saving your changes.

Select All
Click this button to select all check boxes in the window.

Clear All
Click this button to deselect all check boxes in the window.

Report Configuration Form Procedures

The following procedures can be performed on this form.

Add a Report

1. Select ***Reports*** from the ***Administration*** menu. The Reports folder opens.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the report.
4. Click [Browse]. The Open window opens.
5. Select the drive, then the directory, then the file name for an existing report layout.
6. Click [OK] to insert the selection into the **File** field on the Report Configuration form.

Note: You cannot use the Report Configuration form to design a report layout. Only existing layouts can be used to create reports. A valid report layout must have been designed using Crystal Reports for Windows™ and must have the file extension "rpt."

7. In the **Description** field, type a description of this report's contents.
8. If you want to restrict previewing and printing of this report, type a password in the **Password** field.
9. Type the password again in the **Confirm Password** field.
10. In the Type(s) listing window, select the check boxes beside the most appropriate category for this report.

Note: You do not have to select a check box. Many of the reports currently in the system are uncategorized.

11. Click [OK] to add the report. The name of the report will be inserted alphabetically into the listing window.

Modify a Report

1. From the listing window, select the name of the report that you want to be changed. If the report is not listed, make sure that the appropriate check box is selected in the Report View Filter window (displayed by selecting the [Filter Report View] button).
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Note: On Enterprise systems, all servers follow the permissions from the report permission groups. Therefore, if a user has permission to modify a report on a Regional Server, then the user will also have permission to modify the report on the Master Server (and vice versa).

Delete a Report

1. From the listing window, select the name of the report that you want to delete. If the report is not listed, make sure that the appropriate check box is selected in the Report View Filter window (displayed by selecting the [Filter Report View] button).
2. Click [Delete].

3. Click [OK].

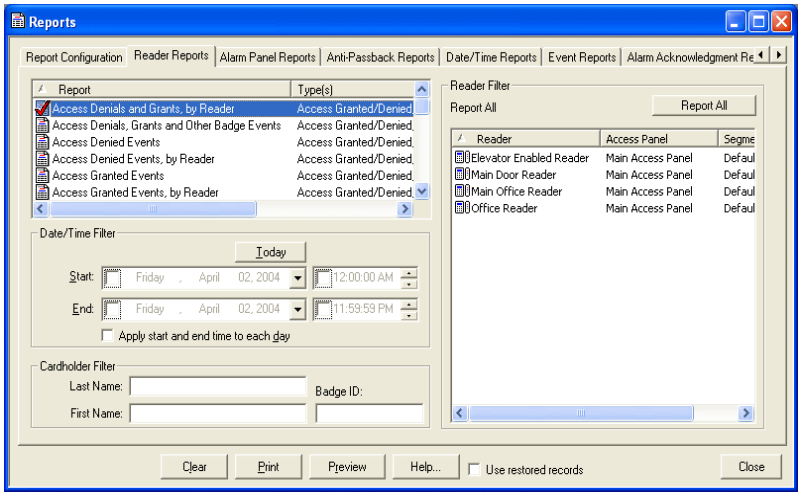
Filter the Report View

1. On the Report Configuration form, click [Filter Report View]. The Report View Filter window opens.
2. Select the check boxes that correspond with the types of reports that you want to view. Click [Select All] to select all of the choices in the listing window. Click [Clear All] to deselect all of the choices in the listing window.
3. Click [OK]. The types of reports that correspond to the check boxes that you selected will be displayed in the listing window on the Report Configuration form.

Preview and Print a Report

For more information, refer to Preview and Print a Report on page 244.

Reader Reports Form



This form allows you to add filtering criteria to a reader report, so that you can narrow the results of your report. Depending on the type of report you select, you can optionally add a filter on reader(s), start date/time, end date/time, badge ID and/or cardholder name.

Listing window

Lists currently defined reader reports that the user is authorized to preview, and each report's type. Note that some reports are categorized under more than one type.

Today

Click this button to set the Start time/date to 12:00:00 AM on the current date or set the End time/date to 11:59:59 PM on the current date

Start

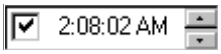
If you want to filter a report by a specific date, select the **Start date** check box and choose a specific start date from the drop-down calendar.

Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the first year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .

Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **Start time** check box and choosing a specific start time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

End

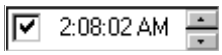
If you want to filter a report by a specific date, select the **End date** check box and choose a specific end date from the drop-down calendar.

Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the last year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .

Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **End time** check box and choosing a specific end time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Apply start and end time to each day

If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM:

If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31.

If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.

Cardholder Filter

Includes the **Last Name**, **First Name**, and **Badge ID** fields. These fields are available only for applicable report types. These fields are not case-sensitive and will match any names beginning with the characters you type (much like the Cardholder form searches). For example, typing “smith” for Last Name will match “Smith”, “SMITHY”, “smithereen”, etc.

Last Name

Enter the cardholder’s last name.

First Name

Enter the cardholder’s first name.

Badge ID

If you wish to report on the activity associated with a specific badge, enter the Badge ID here. This field is available only for applicable report types.

Report All

If this button is pushed, all entries in the Reader list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all readers will be included in the report.

Report All/__ selected

Indicates “Report All” if no devices are selected in the **Reader** field. Indicates “__ selected” if one or more devices are selected in the **Reader** field.

Reader listing window

Lists all readers on the system and the access panel to which each is attached. To select/deselect a reader, click on the icon beside it. A checkmark on an icon indicates that the reader is selected. Only data from selected readers will be included in the report. However, if no devices are selected, data for all readers will be reported.

Clear

Clears all current filter criteria.

Print
Displays the Print Report Options window.

Preview
Displays the selected report with selected criteria in the Report Print Preview window.

Help
Displays relevant on-screen help for this form.

Use restored records
If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current "live" events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information, refer to Chapter 23: Archives Folder on page 501.

Close
Closes the Reports folder.

Reader Reports Form Procedures

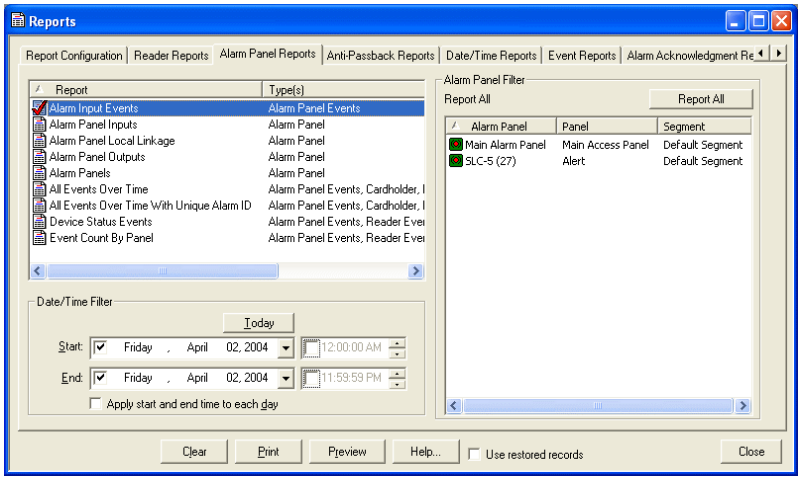
The following procedures can be performed on this form.

Run a Reader Report

1. Select ***Reports*** from the ***Administration*** menu. The Reports folder opens.
2. Select the Reader Reports tab.
3. From the listing window, select the report that you want to run.
4. In the Reader Filter section, select the icon(s) corresponding to the reader(s) whose data you wish to include in the report. If you don't select any readers, data for all readers will be reported.
5. If desired, specify a date/time interval for gathering data in the Date/Time Filter section. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** check box.
6. In the Cardholder Filter section, enter the person's **Last Name**, **First Name**, and/or **Badge ID** if you want the report to contain data pertaining only to cardholders having the specified name and/or badge ID (cardholder name and badge ID is applicable only to reader reports based on events).
7. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 10: Report Print Preview Window on page 241.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Alarm Panel Reports Form



This form allows you to add filtering criteria to an alarm panel report, so that you can narrow the results of your report. Depending on the type of report you select, you can optionally add a filter on alarm panel(s), start date/time, and end date/time.

Listing window

Lists currently defined alarm panel reports that the user is authorized to preview, and each report's type. Note that some reports are categorized under more than one type.

Today

Click this button to set the Start time/date to 12:00:00 AM on the current date or set the End time/date to 11:59:59 PM on the current date

Start

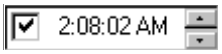
If you want to filter a report by a specific date, select the **Start date** check box and choose a specific start date from the drop-down calendar.

Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the first year for which data is to be included in this report. To change the year, click on the name of the displayed year and use the spin buttons .

Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **Start time** check box and choosing a specific start time.

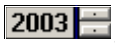


Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

End

If you want to filter a report by a specific date, select the **End date** check box and choose a specific end date from the drop-down calendar.

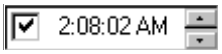
Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the last year for which data is to be included in this report. To change the year, click on the name of the year to access the spin buttons 

.

Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **End time** check box and choosing a specific end time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Apply start and end time to each day

If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM:

If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31.

If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.

Report All

If this button is pushed, all entries in the Alarm Panel list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all readers will be included in the report.

Report All/__ selected

Indicates “Report All” if no devices are selected in the **Alarm Panel** field. Indicates “__ selected” if one or more devices are selected in the **Alarm Panel** field.

Alarm Panel listing window

Lists all alarm panels on the system and the access panel to which each is attached. To select/deselect an alarm panel, click on the icon beside it. A checkmark on an icon indicates that the alarm panel is selected. Only data from selected alarm panels will be included in the report. However, if no devices are selected, data for all alarm panels will be reported.

Clear

Clears all current filter criteria.

Print

Displays the Print Report Options window.

Preview

Displays the selected report with selected criteria in the Report Print Preview window.

Help

Displays relevant on-screen help for this form.

Use restored records

If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information, refer to Chapter 23: Archives Folder on page 501.

Close

Closes the Reports folder.

Alarm Panel Reports Form Procedures

The following procedures can be performed on this form.

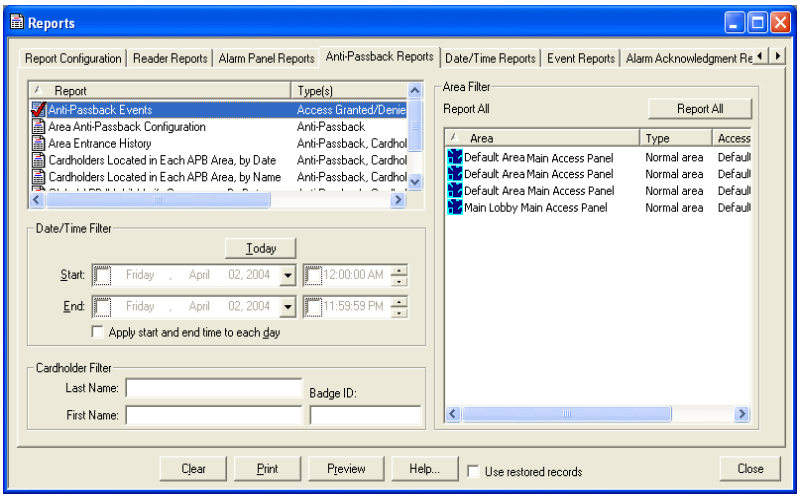
Run an Alarm Panel Report

1. Select ***Reports*** from the ***Administration*** menu. The Reports folder opens.
2. Select the Alarm Panel Reports tab.
3. From the listing window, select the report that you want to run.
4. If desired, specify a date/time interval for gathering data in the Date/Time Filter section. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** check box.

5. In the Alarm Panel Filter section, select the icon(s) corresponding to the alarm panel(s) whose data you wish to include in the report. If you don't select any alarm panels, or click [Report All], data for all alarm panels will be reported.
6. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 10: Report Print Preview Window on page 241.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Anti-Passback Reports Form



This form allows you to add filtering criteria to an anti-passback report, so that you can narrow the results of your report. Depending on the type of report you select, you can optionally add a filter on area(s), start date/time, end date/time, badge ID and/or cardholder name.

Listing window

Lists currently defined anti-passback reports, and each report(s) type. Note that some reports are categorized under more than one type.

Today

Click this button to set the Start time/date to 12:00:00 AM on the current date or set the End time/date to 11:59:59 PM on the current date.

Start

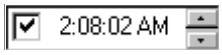
If you want to filter a report by a specific date, select the **Start date** check box and choose a specific start date from the drop-down calendar.

Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the first year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .

Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **Start time** check box and choosing a specific start time.

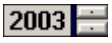


Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

End

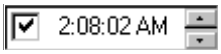
If you want to filter a report by a specific date, select the **End date** check box and choose a specific end date from the drop-down calendar.

Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the last year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons  .

Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **End time** check box and choosing a specific end time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Apply start and end time to each day

If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM:

If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31.

If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.

Cardholder Filter

Includes the **Last Name**, **First Name**, and **Badge ID** fields. These fields are available only for applicable report types. These fields are not case-sensitive and will match any names beginning with the characters you type (much like the Cardholder form searches). For example, typing “smith” for Last Name will match “Smith”, “SMITHY”, “smithereen”, etc.

Last Name

Enter the cardholder’s last name.

First Name

Enter the cardholder’s first name.

Badge ID

If you wish to report on the activity associated with a specific badge, enter the Badge ID here. This field is available only for applicable report types.

Report All

If this button is pushed, all entries in the Area list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all areas will be included in the report.

Report All/__ selected

Indicates “Report All” if no entries are selected in the **Area** field. Indicates “__ selected” if one or more entries are selected in the **Area** field.

Area listing window

Lists all anti-passback areas defined on the system, and the access panel associated with each. To select/deselect an area, click on the icon beside it. A checkmark on an icon indicates that the area is selected. Only data pertaining to selected areas will be included in the report. However, if no entries are selected, data for all areas will be reported.

Clear

Clears all current filter criteria.

Print

Displays the Print Report Options window.

Preview
Displays the selected report with selected criteria in the Report Print Preview window.

Help
Displays relevant on-screen help for this form.

Use restored records
If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder.

Close
Closes the Reports folder.

Anti-Passback Reports Form Procedures

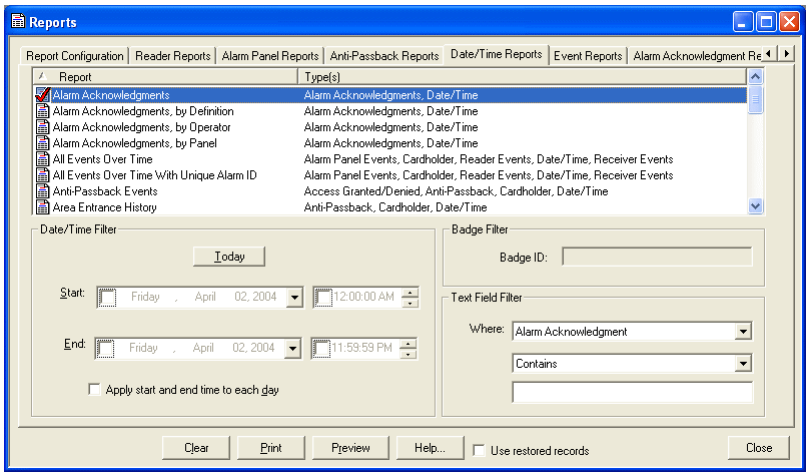
The following procedures can be performed on this form.

Run an Anti-Passback Report

1. Select ***Reports*** from the ***Administration*** menu. The Reports folder opens.
2. Select the Anti-Passback Reports tab.
3. In the reports listing window, select the icon that corresponds to the report you wish to run.
4. Complete the Date/Time Filter section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** check box.
5. In the Cardholder Filter section, enter the person’s **Last Name**, **First Name**, and/or **Badge ID** if you want the report to contain data pertaining only to cardholders having the specified name or badge ID.
6. In the Area Filter section, select the icon(s) corresponding to the anti-passback area(s) whose data you wish to include in the report. If you don’t select any areas, or click [Report All], data for all areas will be reported.
7. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 10: Report Print Preview Window on page 241.

Note: Only data that’s currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Date/Time Reports Form



This form allows you to add filtering criteria to a date/time report, so that you can narrow the results of your report.

Listing window

Lists currently defined date/time reports that the user is authorized to preview, and each report(s) type. Note that some reports are categorized under more than one type.

Today

Click this button to set the Start time/date to 12:00:00 AM on the current date or set the End time/date to 11:59:59 PM on the current date.

Start

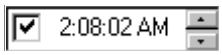
If you want to filter a report by a specific date, select the **Start date** check box and choose a specific start date from the drop-down calendar.

Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the first year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .

Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **Start time** check box and choosing a specific start time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

End

If you want to filter a report by a specific date, select the **End date** check box and choose a specific end date from the drop-down calendar.

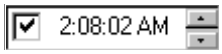
Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the last year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons

.

Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **End time** check box and choosing a specific end time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Apply start and end time to each day

If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM:

If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31.

If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.

Badge ID

If you wish to report on the activity associated with a specific badge, enter the Badge ID here. This field is available only for applicable report types.

Text Field Filter

Includes the **Where** and **Match criteria** fields, as well as a **Blank field**. This section is enabled only when a report that allows filtering is selected in the listing window.

Where

You can now add a text filter to the following:

- Action Type, Details, or Object for User Transactions reports
- Alarm Acknowledgment text for Alarm Acknowledgments reports

When this section is enabled, the **Where** field contains the attribute in OnGuard that is to be filtered.

Match criteria (Set to Contains by default. May also be set to Begins With, Ends With, or Equals)

If enabled, the **Match criteria** drop-down list may be changed from its default value of contains to Begins With, Ends With, or Equals. This setting specifies how the selection in the **Where** field relates to the value entered to search for in the **Blank field**.

Blank field

In this field, type the value you wish to filter or search for. For example, if you wanted to display all User Transactions associated with System Administration, you should:

1. Select a User Transaction Log report in the listing window.
2. In the **Where** field, select “Object”.
3. In the **Match criteria** field, select “Equals”.
4. In the blank field, type “System Administration” (without the quotes).
5. Click [Preview], and only those entries associated with System Administration will be displayed in the resulting report.

Clear

Clears all current filter criteria.

Print

Displays the Print Report Options window.

Preview

Displays the selected report with selected criteria in the Report Print Preview window.

Help

Displays relevant on-screen help for this form.

Use restored records

If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information, refer to Chapter 23: Archives Folder on page 501.

Close

Closes the Reports folder.

Date/Time Reports Form Procedures

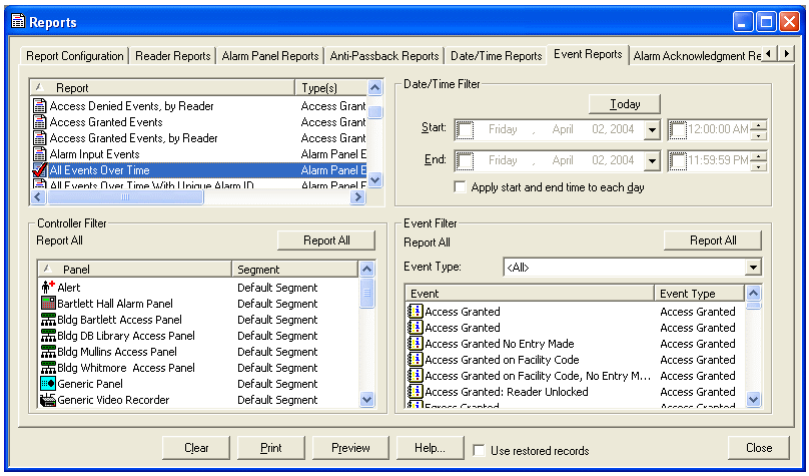
The following procedures can be performed on this form.

Run a Date/Time Report

1. Select ***Reports*** from the ***Administration*** menu. The Reports folder opens.
2. Select the Date/Time Reports tab.
3. In the reports listing window, select the icon that corresponds to the report you wish to run.
4. Complete the Date/Time Filter section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** check box.
5. Enter a **Badge ID** if you want the report to contain data pertaining only to cardholders having the specified name or badge ID.
6. Complete the Text Field Filter section. (This section is optional, and is only enabled for User Transactions reports and Alarm Acknowledgment reports.)
   a. Select a value to filter in the **Where** field.
      - If the report you are running is a User Transactions report and you wish to apply a filter, select Action Type, Details, or Object in the **Where** field.
      - If the report you are running is an Alarm Acknowledgment report and you wish to apply a filter, select Alarm Acknowledgment in the **Where** field.
   b. In the next drop-down list, select whether the filter criteria **Begins With**, **Contains**, **Ends With** or **Equals** the value that you will enter in the next blank field.
   c. In the blank field, type the value you wish to filter for.
7. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 10: Report Print Preview Window on page 241.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Event Reports Form



On the Event Reports form, any report in the reports listing window that has “Cardholder” listed in the Type(s) column is available on the Reports form in the Cardholders folder. This means that a report can be generated on the Reports form in the Cardholders folder based on a cardholder search operation.

This form allows you to add filtering criteria to an event report, so that you can narrow the results of your report.

Listing window

Lists currently defined event reports that the user is authorized to preview, and each report’s type(s). Note that some reports are categorized under more than one type.

Today

Click this button to set the Start time/date to 12:00:00 AM on the current date or set the End time/date to 11:59:59 PM on the current date.

Start

If you want to filter a report by a specific date, select the **Start date** check box and choose a specific start date from the drop-down calendar.

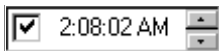
Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the first year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons

.

Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **Start time** check box and choosing a specific start time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

End

If you want to filter a report by a specific date, select the **End date** check box and choose a specific end date from the drop-down calendar.

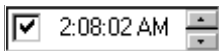
Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the last year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons

.

Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **End time** check box and choosing a specific end time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Apply start and end time to each day

If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM:

If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31.

If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.

Report All (panels)

If this button is pushed, all entries in the Panel list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all access panels will be included in the report.

Report All/__ selected

Indicates “Report All” if no entries are selected in the **Panel** field. Indicates “__ selected” if at least one entry is selected in the **Panel** field.

Panel listing window

Lists all panels in the system. An icon that indicates the panel’s type precedes each entry. If your installation uses segmentation, the segment assignment is listed for each entry.

Report All (events)

If this button is pushed, all entries in the Event list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all events for the selected **Event Type** will be included in the report.

Report All/__ selected

Indicates “Report All” if no entries are selected in the **Event** field. Indicates “__ selected” if at least one entry is selected in the **Event** field.

Event Type

Can be used to filter all events of a particular type. For example, if you select the “All Events Over Time” report and select an **Event Type** of “Fire”, an “All Fire Events Over Time” report will effectively be created.

Event listing window

Lists currently defined events for the selected **Event Type**, and each event’s type.

Clear

Clears all current filter criteria.

Print

Displays the Print Report Options window.

Preview

Displays the selected report with selected criteria in the Report Print Preview window.

Help

Displays relevant on-screen help for this form.

Use restored records

If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information, refer to Chapter 23: Archives Folder on page 501.

Close

Closes the Reports folder.

Event Reports Form Procedures

The following procedures can be performed on this form.

Run an Event Report

1. Select ***Reports*** from the ***Administration*** menu. The Reports folder opens.
2. Select the Event Reports tab.
3. In the reports listing window, select the icon that corresponds to the report you wish to run.
4. Complete the Date/Time Filter section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** check box.
5. In the Access Panel Filter section, select the icon(s) corresponding to the panel(s) whose data you wish to include in the report. If you don't select any panels, or click [Report All], data for all panels will be reported.
6. In the Event Filter section, select an **Event Type**.
7. In the Event listing window, select the icon(s) corresponding to the event(s) whose data you wish to include in the report.
   - If you select "<All>" in the **Event Type** field, data for all events will be reported.
   - If you click [Report All], data for all events of the selected **Event Type** will be reported.
8. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 10: Report Print Preview Window on page 241.

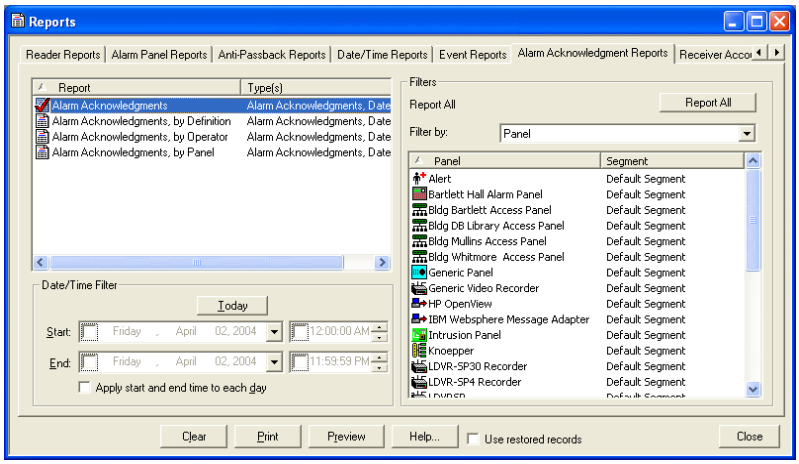
Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Alarm Acknowledgment Reports Form

The Alarm Acknowledgment Reports form is designed to provide reports on acknowledged alarms. These reports can be filtered by the date/time the acknowledgment occurred, the device that triggered the alarm, and the operator who acknowledged the alarm. When you select a filter, the report displays alarm acknowledgments for only the filtered device. If you want to view everything, use the convenient [Report All] button.

The result of the report includes the following:

- Date and time this report was created
- Date and time the alarm occurred
- Date and time the alarm was acknowledged
- Who acknowledged the alarm
- Any notes included with the acknowledgment
- The device that caused the alarm
- The total number of acknowledgments



Notes: The details column does not report who acknowledged the alarm, but rather who was logged into Alarm Monitoring when the alarm was acknowledged. Therefore, someone other than the person logged into Alarm Monitoring may have acknowledged the alarm.

The first and last name displayed in the details column are configured in the System Administration Users folder.

Listing window

Lists currently defined alarm acknowledgment reports that the user is authorized to preview, and each report's type(s). Note that some reports are categorized under more than one type.

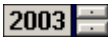
Today

Click this button to set the Start time/date to 12:00:00 AM on the current date or set the End time/date to 11:59:59 PM on the current date

Start

If you want to filter a report by a specific date, select the **Start date** check box and choose a specific start date from the drop-down calendar.

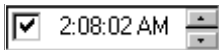
Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the first year for which data is to be included in this report. To change the year, click on the name of the displayed year to access the spin buttons  .

Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Start

Select the time for which data is to be included in this report by selecting the **Start time** check box and choosing a specific start time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

End

If you want to filter a report by a specific date, select the **End date** check box and choose a specific end date from the drop-down calendar.

Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

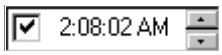
Select the last year for which data is to be included in this report. To change the year, click on the name of the year to access the spin buttons

.

End

Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **End time** check box and choosing a specific end time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Apply start and end time to each day

If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM:

If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31.

If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.

Report All
Reports every alarm acknowledgment and does not apply any filter.

Filter by
Select one device you want the report based on. The report displays the alarm acknowledgments only for the device you select.

Filter listing window
Select one or multiple filters for the report. The filters that display in this window depend on what you select in the **Filter by** drop-down list. The report displays the alarm acknowledgments for only the devices you select.

Clear
Clears all current filter criteria.

Print
Displays the Print Report Options window.

Preview
Displays the selected report with selected criteria in the Report Print Preview window.

Help
Displays relevant on-screen help for this form.

Use restored records
If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current "live" events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information, refer to Chapter 23: Archives Folder on page 501.

Close
Closes the Reports folder.

Alarm Acknowledgment Reports Form Procedures

The following procedures can be performed on this form.

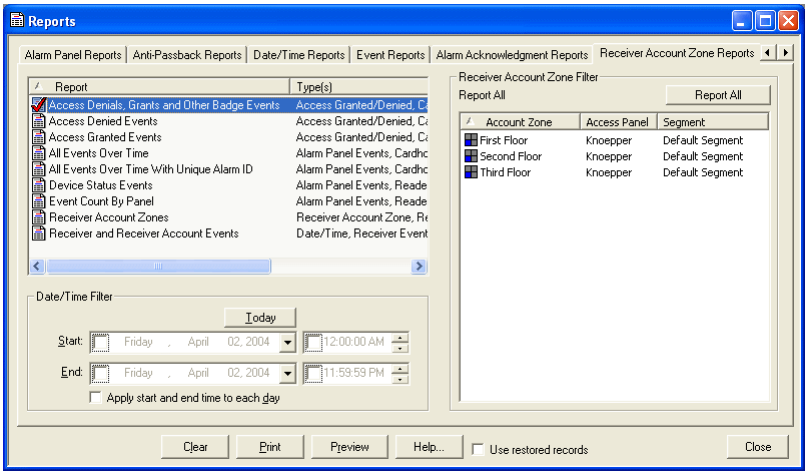
Run an Alarm Acknowledgment Report

1. Select ***Reports*** from the ***Administration*** menu. The Reports folder opens.
2. Select the Alarm Acknowledgment Reports tab.
3. In the listing window, select the report you wish to run.
4. Complete the Date/Time Filter section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** check box.
5. In the **Filter by** drop-down list, select the device whose data you wish to include in the report. If you don't select any device, or if you click [Report All], data for every device will be reported.
6. In the Filter listing window, select the device(s) whose data you wish to include in the report.

7. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 10: Report Print Preview Window on page 241.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Receiver Account Zone Reports Form



This form allows you to add filtering criteria to a receiver account zone report, so that you can narrow the results of your report.

Listing window

Lists currently defined alarm acknowledgment reports that the user is authorized to preview, and each report's type(s). Note that some reports are categorized under more than one type.

Today

Click this button to set the Start time/date to 12:00:00 AM on the current date or set the End time/date to 11:59:59 PM on the current date

Start

If you want to filter a report by a specific date, select the **Start date** check box and choose a specific start date from the drop-down calendar.

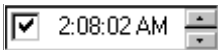
Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the first year for which data is to be included in this report. To change the year, click on the name of the displayed year to access the spin buttons .

Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Start

Select the time for which data is to be included in this report by selecting the **Start time** check box and choosing a specific start time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

End

If you want to filter a report by a specific date, select the **End date** check box and choose a specific end date from the drop-down calendar.

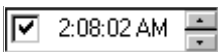
Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.

Select the first year for which data is to be included in this report. To change the year, click on the name of the displayed year to access the spin buttons .

End

Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Select the time for which data is to be included in this report by selecting the **End time** check box and choosing a specific end time.



Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Apply start and end time to each day

If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM:

If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31.

If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.

Report All (account zones)

If this button is pushed, all entries in the Account Zone list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all account zones will be included in the report.

Report All/___ selected

Indicates “Report All” if no entries are selected in the **Account Zone** field. Indicates “__ selected” if at least one entry is selected in the **Account Zone** field.

Account Zone listing window

Lists all account zones in the system. An icon that indicates the account zone’s type precedes each entry. If your installation uses segmentation, the segment assignment is listed for each entry.

Clear

Clears all current filter criteria.

Print

Displays the Print Report Options window.

Preview

Displays the selected report with selected criteria in the Report Print Preview window.

Help

Displays relevant on-screen help for this form.

Use restored records

If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information, refer to Chapter 23: Archives Folder on page 501.

Close

Closes the Reports folder.

Receiver Account Zone Reports Form Procedures

The following procedures can be performed on this form.

Run a Receiver Account Zone Report

1. Select ***Reports*** from the ***Administration*** menu. The Reports folder opens.
2. Select the Receiver Account Zone Reports tab.
3. In the listing window, select the icon that corresponds to the report you wish to run.
4. Complete the Date/Time Filter section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** check box.
5. In the Account Zone Filter section, select the icon(s) corresponding to the account zone(s) whose data you wish to include in the report. If you don't select any account zones, or if you click [Report All], data for all account zones will be reported.
6. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 10: Report Print Preview Window on page 241.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

CHAPTER 9

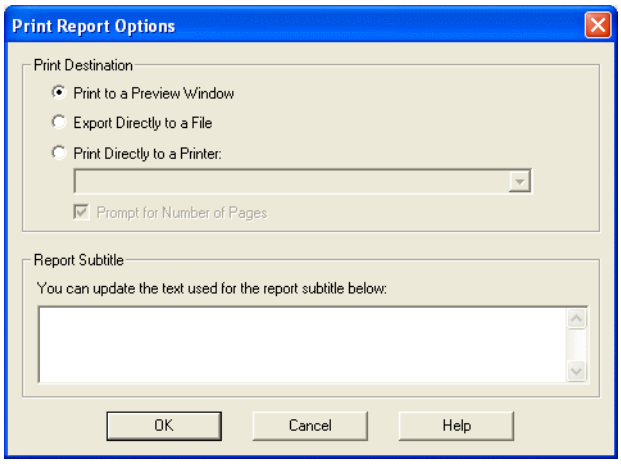
Print Report Options Window

From the Print Report Options window, you can:

- Choose a destination for the report. Choices include:
  - Preview Window (the default)
  - Direct Export to a File
  - Directly to a Printer
- Update the subtitle used for the report

This window is displayed by clicking the [Print] button

Print Report Options Window



Print Destination

Includes the **Print to a Preview Window**, **Export Directly to a File** and **Print Directly to a Printer** radio buttons. Also includes the **Printer** drop-down list and the **Prompt for Number of Pages** check box.

Print to a Preview Window

If selected, the Report Print Preview window will be displayed when the [OK] button is clicked. In the Report Print Preview window, you can view the selected report on the screen.

For more information, refer to Chapter 10: Report Print Preview Window on page 241.

Export Directly to a File

If selected, the Export window will be displayed when the [OK] button is clicked. Choose the report Format and Destination from the drop-down lists.

Depending on what you choose, enter the destination and format information in the corresponding window, then click [OK].

Print Directly to a Printer

If selected, also select a printer from the Printer drop-down list.

If you select the **Prompt for Number of Pages** check box, the Print window will be displayed where you can select the print range, number of copies and whether or not to collate your report.

Printer drop-down list

Select a printer in this field for the report to be printed on. This field is enabled for selection only when the **Print Directly to a Printer** radio button is selected.

All printers currently configured for use are listed.

Prompt for Number of Pages

This field is enabled for selection only when the **Print Directly to a Printer** radio button is selected.

If selected, the Print window will be displayed where you can select the print range, number of copies and whether or not to collate your report.

Report Subtitle textbox

Type the text here that will be displayed as the subtitle on the report.

OK

Prints the report using the options you selected.

Cancel

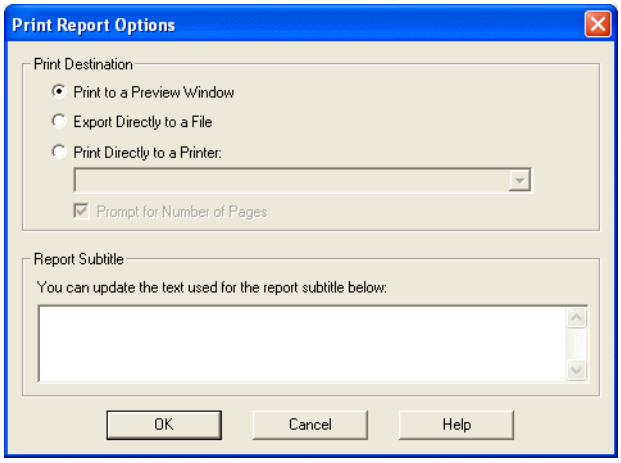
Closes the Print Report Options window without printing the report.

Help

Displays online help for this form.

Print a Report

1. Select a report from within the Reports folder.
2. The Print Report Options window opens.



3. In the Print Destination section, select whether to print to a preview window, export directly to a file or print directly to a printer.
4. If you selected **Print Directly to a Printer** in the Print Destination section, select a printer in the drop-down list and choose whether to **Prompt for Number of Pages**.

Note: If the Linkage Server is running under a local system account it may not have permission to access a network printer (depending on its configuration). If this is the case you must select a local or default network printer. Contact your System Administrator to determine what account the Linkage Server is running under and the printers it can access.

5. In the Report Subtitle section, type the report subtitle. The subtitle will be displayed below the report title on the report.
6. Click [OK]. The options selected in the Print Destination section will determine where the report is sent.

CHAPTER 10

Report Print Preview Window

From the Report Print Preview window, you can:

- View an on-screen report created.
- Print a report, save it to a file or send it over electronic mail.
- Search for any textual information in the report.

If you click [Preview] or [Print Preview] while a report form is displayed, the report is automatically printed to the Report Print Preview window.

This window is displayed by:

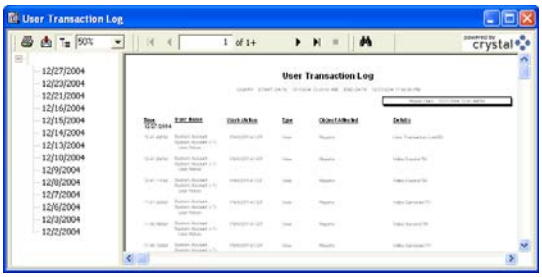
- Clicking on the [Print Preview] button on any form in the Reports folder.
- Clicking on the Print Preview toolbar button when a report is selected on a form in the Reports folder.

Toolbar Shortcut

- Clicking [Print] , selecting the **Print to a Preview Window** radio button on the Print Report Options window, then clicking the [OK] button. (This is how the Report Print Preview form can be viewed from the Reports form in the Cardholders folder, the Visits folder or the Assets folder.)

Toolbar Shortcut

Report Print Preview Window



Report navigation tree

The display in the left portion of the Report Print Preview window. The report navigation tree lists the records contained in the report, in a hierarchical arrangement. The information is content-sensitive. The report type determines the entries in the tree.

For example, the default “User Transaction Log” report is arranged in date order, so the tree will contain a list of dates. The tree for the default “Text Instructions” report lists alarms. The “Access and Denials, by Reader” report has an entry for each queried reader, with subentries by event date.

If the tree has branching entries, you can expand the branches of the tree. When you click an entry in the tree, you move to that section or record in the report. When a section or record is selected via the report navigation tree, that section or record will appear in the preview window with a blue box border. For more information, refer to Preview and Print a Report on page 244.

Preview window

The display in the right portion of the Report Print Preview window. The preview window displays up to one full page of the report, depending upon the zoom level set. If a report appears too large for the current window, either adjust the zoom level or use the up, down, left, and right arrow keys to scroll and see the rest of that page of the report.

For reports that contain more than one page, use the arrows or the <Page Up>/<Page Down> keys to navigate through the pages.

Print

Click to display a Print window from where you can select the page range and number of copies to print, then initiate report printing.

Export

Click to export the report to a file or to your organization’s electronic mail system.

Navigation Tree

Click to toggle the display of the report navigation tree on or off.

Zoom

From this drop-down list, you can select the magnification level of the preview window contents, with respect to the actual size. Choices include 400%, 300%, 200%, 150%, 100%, 75%, 50%, 25%, Page Width and Whole Page. Selecting either Page Width or Whole Page displays the corresponding percentage in this field. You can also type a number directly into this field, but you must then either press <Tab> or click outside of the field for the number to take effect.

First

Click to move to the first page of the report.

Previous

Click to move to the previous page of the report. Another way to do this is to click the <Page Up> key.

Page count

This display indicates the page number of the currently displayed page, followed by the total page count for the report. For example: “2 of 4.”

Next

Click to move to the next page of the report. Another way to do this is to click the <Page Down> key.

Last

Click to move to the last page of the report.

Stop

Click to terminate the report building process. This button is especially useful if the report is lengthy and you want to view only part of it.

Search

Click to display the Search window from where you can perform a text search of the report. When you enter text in the **Find what** field (in the Search window) and click [Find Next], the view jumps to the first occurrence of the requested text or a message is displayed if no match was found.

Report Print Preview Window Right-click Options

While viewing a report in the Report Print Preview Window there are a number of right-click options and identifiers that appear depending on what section of the report is highlighted.

- **Field**: Tells you what field is currently selected.
- **Text**: Tells you whether the current selection is text.
- **Copy**: Copy the information into the clipboard.
- **Freeze Pane**: Freezes the section of the pane so you continue to see the information as you scroll.
- **Unfreeze Pane**: Unfreezes the pane so the page scrolls normally

Report Print Preview Window Procedures

Use the following procedures in this window.

Preview and Print a Report

1. Select a report from within the Reports folder.

   Note: Reports are also available on the Reports form in the Cardholders folder, Visits folder and Assets folder. However, the Print Preview toolbar button and the [Preview] button on the form are disabled or "grayed out." Instead, the Print toolbar button or the [Print] button on the form are used to preview and print reports from these forms. For more information, refer to Print a Report on page 238.

2. Select additional criteria if you want the report to include only a specific range of data.
3. Click one of the following:
   - The [Print] button, select the **Print to a Preview Window** radio button and then click [OK].
   - The [Preview] button on the form.
4. The Report Print Preview window is displayed.
   - On the left, the report navigation tree may have branching entries.
     - If the tree has branching entries, expand that branch of the tree.
     - Click an entry in the tree to move to that section or record in the report. When a section or record is selected via the report navigation tree, that section or record will appear in the preview window with a blue box border.
   - On the right, the preview window will show the first page of the report as it will look when it is printed. Click a section or record in the preview window. When a section or record is selected in the preview window, that section or record will appear in the preview window with a blue box border.
   - Click and drag the split bar to resize the report navigation tree and the preview window relative to each other.
   - Click the button to hide the report navigation tree and maximize the space used for the preview window.
5. Use the , , and buttons or the <Page Down>/<Page Up> keys to view other pages of the report.
6. Select an option from the zoom drop-down list to change the size of the display. You can instead type a number directly into this field, but you must then either press <Tab> or click outside of the field for the number to take effect. If a report page is still too large for the window, you can use the up, down, left, and right arrow keys to scroll and see the rest of the page.
7. To save the report to a file on your computer or to send the report to someone using your company's electronic mail system, select the button. The Export window is displayed.
   - Select the format that you want to send the report in from the **Format** drop-down list.
   - In the **Destination** drop-down list, you can choose to export the report to an application, a disk file, an exchange folder, a Lotus Notes database or your electronic mail system (if you have one).
   - Click [OK] and follow the instructions
8. To print the report from within the Report Print Preview window:
   a. Click the button. The Print window is displayed from where you can select which pages to print and the number of copies.
   b. Select one of the following:

- The **All** radio button to print the entire report without user intervention.
- The **Pages** radio button and enter a page range.

c. A message box will be displayed to indicate the status of the print operation.

Search a Report for Specific Information

1. To search through the report for specific information, click the button.
2. The Search window is displayed. In the **Find what** field, type the word, contiguous words or number you wish to locate in the report.

Note: The search is not case-sensitive.

3. Click [Find Next].
4. One of two things will happen:
   - If the requested information was found, the preview window display will move to the first occurrence of it.
   - If the information is not contained in the report, a message box will be displayed.
5. If the requested information was found, click [Find Next] to move through successive occurrences of it.

CHAPTER 11

Card Formats Folder

The Card Formats folder contains forms with which you can:

- Specify format parameters for magnetic, Wiegand and smart card formats
- Specify required fields for cardholder records of a given badge type

The Card Formats folder contains two forms if your system is not segmented: the Card Format and Custom Encoding form. If you system is segmented, the Card Formats folder contains a third form, the Segment Membership form.

Note: Card formats can be segmented. Card format segmentation is more flexible than segmentation of other hardware-related items. When card format segmentation is enabled, a card format can belong to <All Segments> (system-wide), one segment, or many segments.

This folder is displayed by selecting ***Card Formats*** from the ***Administration*** menu, or by selecting the Card Formats toolbar button.

Toolbar Shortcut

Card Format Form - Common Fields

The following table lists the common fields found in the Card Format form, regardless of whether you are working with magnetic, Wiegand, or smart card formats.

Listing window
Lists currently defined card formats, the type of card, segment, and, ID number.

Name
A unique name for the specified card format. You can enter a name containing a maximum of 32 characters.

Type
Displays the card format type. The information in this field represents the selection made in the Choose Card Format Type window when the card format was added. This field is automatically populated and cannot be modified.

Add
Adds a card format entry.

Modify
Changes a card format entry.

Delete
Removes a smart card format entry.

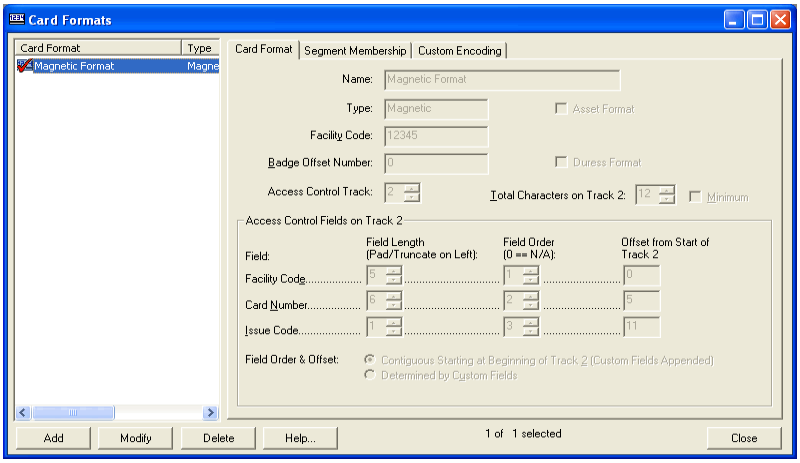
Help
Displays online help for this topic.

Close
Closes the Card Formats folder.

Magnetic Card Format Form

You can use the Magnetic Card Format form to:

- Configure magnetic card formats.
- Define information for the magnetic stripe, including the order and size of fields, the unique facility code, and, the number of digits to be encoded on the card.



Facility Code
Specifies a unique value for this facility.

Badge Offset Number
The **Badge Offset Number** field is utilized in the card format configuration to offset the badge number by the value entered in the field.

An example would be: if the actual card badge number is 1500 and the **Badge Offset Number** field is set to 1000 then the number reported in the access event would 2500. This is useful to keep

duplicate badge ID's unique. When multiple independent systems are merged into one OnGuard system duplicate badge ID's could become a problem. It is important that the access control hardware is able to uniquely identify the card format using the offset by a different facility code or card format structure.

If the Badge Offset Number is set to zero (0) then no offset is applied and the actual badge number is reported.

Access Control Track

Selects the track for which to configure access control. The default is track 2.

Asset Format

When this box is checked, the selected card format can be configured for asset management.

Note: The **Asset Format** check box should not be selected if the access levels associated with the badge has escort functionality.

Duress Format

Identifies this card format as a duress format. When the controller detects a duress format, it always reports the events as duress rather than normal.

Note: This setting is ignored during badge encoding.

This setting is different than the **Deny On Duress PIN** setting for readers which accept PIN input. For more information, refer to Settings Form on page 645.

Total Characters on Track n

Specifies the total number of digits for all fields (including custom) on the access control track. You can choose a value in the range of 0 through 100.

Minimum

When this box is checked, the total number of characters on the specified track can vary as long as the number of characters exceeds the minimum length entered in the **Total Characters on Track n** field. Data will be right-padded with zeroes until the minimum length is reached.

When this box is unchecked, the total number of characters on the specified track is the exact number specified in the **Total Characters on Track n** field.

Field Length: Facility Code

Specifies the maximum number of digits the facility code can contain. You can choose a value in the range of zero through nine. A facility code shorter than the value will be padded with leading zeroes (zeroes will be inserted in front of it).

Field Length: Card Number

Specifies the maximum number of digits the card number can contain. You can choose a value in the range of zero through nine. A card number shorter than the value will be padded with leading zeroes (zeroes will be inserted in front of it).

Field Length: Issue Code

Specifies the maximum number of digits the issue code can contain. You can choose a value in the range of zero through two. An issue code shorter than the value will be padded with leading zeroes (zeroes will be inserted in front of it).

Field Order (0 = N/A)

Contains the **Field Order: Facility Code**, **Field Order: Card Number**, and **Field Order: Issue Code** fields. If you select the **Determined by Custom Fields** radio button, this section is dimmed because the field order will be specified in the custom encoding view instead.

An access control field is not encoded if the value of the field order equals zero.

Field Order: Facility Code

Indicates the position of this field on the access control track, with respect to the card number and issue code. Choose one of the following:

- 1 = placed first on the card
- 2 = placed second on the card
- 3 = placed last on the card
- 0 = N/A

No two fields can have the same number. The exception to this is choice “0”— more than one of the fields can be assigned “0”.

Field Order: Card Number

Indicates the position of this field on the access control track, with respect to the facility code and issue code. Choose one of the following:

- 1 = placed first on the card
- 2 = placed second on the card
- 3 = placed last on the card
- 0 = N/A

No two fields can have the same number. The exception to this is choice “0”— more than one of the fields can be assigned “0”.

Field Order: Issue Code

Indicates the position of this field on the access control track, with respect to the card number and facility code. Choose one of the following:

- 1 = placed first on the card
- 2 = placed second on the card
- 3 = placed last on the card
- 0 = N/A

No two fields can have the same number. The exception to this is choice “0”— more than one of the fields can be assigned “0”.

Offset from Start of Track n: Facility Code

This field is updated automatically and is based on the field length and field order values; you cannot change it. It specifies the first character position for encoding the facility code on the magnetic stripe, as measured from the beginning of the access control track.

Offset from Start of Track n: Card Number

This field is updated automatically and is based on the field length and field order; you cannot change it. This field specifies the first character position for encoding the card number on the magnetic stripe, as measured from the beginning of the access control track.

Offset from Start of Track n: Issue Code

This field is updated automatically and is based on the field length and field order; you cannot change it. This field specifies the first character position for encoding the issue code on the magnetic stripe, as measured from the beginning of the access control track.

Field Order & Offset

Determines whether the position of the access control fields (facility code, card number, and, issue code) on the access control track is on the Card Format form or the Custom Encoding form.

Contains the **Contiguous Starting at Beginning of Track n (Custom Fields Appended)** and **Determined by Custom Fields** radio buttons.

Add a Magnetic Card Format

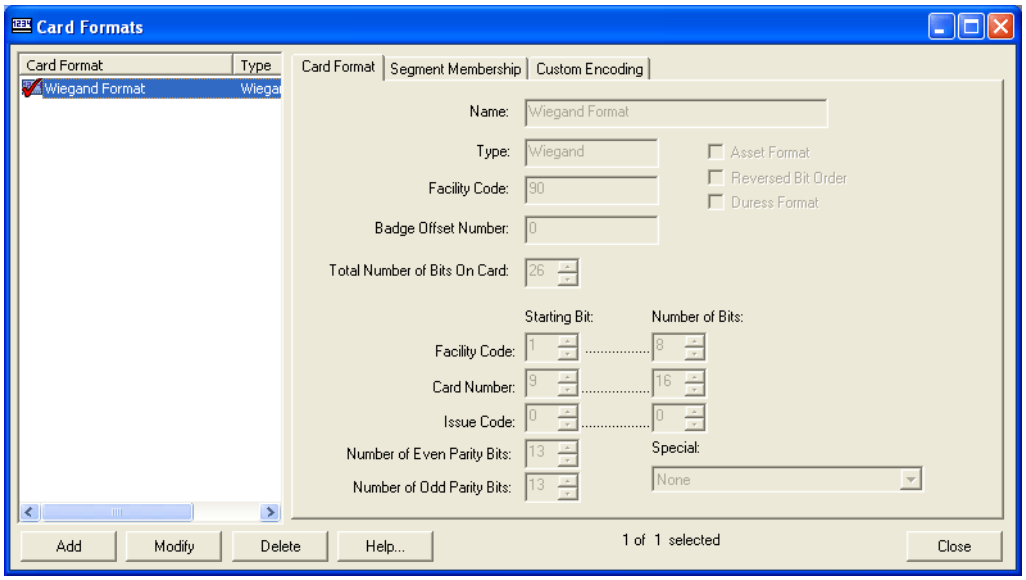
Your system can support a maximum of eight magnetic card formats. This is a limitation of existing hardware.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select **Magnetic** and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. If you want cards with this format to be available for asset assignment, select the **Asset Format** check box.
7. If you want cards with this format to be duress cards, select the **Duress Format** check box.
8. Enter the facility code for this format, if there is one.
9. If your system uses multiple card technologies with overlapping card numbers, specify an offset in the **Badge Offset Number** field.
10. In the **Access Control Track** field, select the track for which to configure access control.
11. In the **Total Characters on Track n** field, select the total number of digits for all fields (including custom) on the access control track.
12. Select the **Minimum** check box if you want the total characters on the track to be a minimum value. Uncheck the **Minimum** check box if you want the total characters on the track to be an exact value.
13. For the facility code, card number, and issue code, indicate the field length of each field.
14. Specify the access control track field order for facility code, card number, and issue code, or select the **Determined by Custom Fields** radio button.

Note: If you want to custom encode, click the Custom Encoding form. For more information, refer to Build a Custom Expression: Process Outline on page 299.

15. Click [OK].

Wiegand Card Format Form



Asset Format

When this box is checked, the selected card format can be configured for asset management. The **Asset Format** check box should not be selected if the access levels associated with the badge has escort functionality.

Reversed Bit Order

This option is supported only in series 2 Lenel access panels. Identifies this card format as a reversed bit order format. When the controller detects this format, it reverses the bit order of the incoming data before processing it.

Readers report the duress state differently. For example, Bioscrypt readers report duress by reversing the bit order of the entire Wiegand string longitudinally.

This setting is ignored during badge encoding.

Duress Format

(This option is supported only in series 2 Lenel access panels.) Identifies this card format as a reader duress card format. When the controller receives a duress format from the reader, it reports the access related events as duress followed by the access event description rather than normal standard reporting. For example: “DURESS - Access Grant” vs. “Access Grant”.

Note: This setting is ignored during badge encoding.

This setting is different than the **Deny On Duress PIN** setting for readers that accept PIN input. The deny on duress reader setting only functions using this setting and not the duress card format. For more information, refer to Settings Form on page 645.

Facility Code

Specifies a unique value for this facility. Choose a value less than 999999999.

Badge Offset Number

The **Badge Offset Number** field is utilized in the card format configuration to offset the badge number by the value entered in the field.

An example would be: If the actual card badge number is 1500 and the **Badge Offset Number** field is set to 1000 then the number reported in the access event would 2500. This is useful to keep duplicate badge ID's unique. When multiple independent systems are merged into one OnGuard system duplicate badge ID's could become a problem. It is important that the access control hardware is able to uniquely identify the card format using the offset by a different facility code or card format structure.

If the Badge Offset Number is set to zero (0) then no offset is applied and the actual badge number is reported.

Choose a value less than 999999999.

Total Number of Bits On Card

The total number of bits encoded on the card with a maximum value of 256 bits.

The number of bits in **Facility Code**, **Issue Code**, and **Card Number** combined must not exceed the total number of bits on the card. If one or more fields are out of range, the system will reset them to the maximum bits allowed.

Except for the parity bits, the fields should not overlap and the length of a field cannot extend beyond the length of the card.

Starting Bit for Facility Code

The bit number on which the facility code begins. Choose a starting value from 0 - 255.

Starting Bit for Card Number

The bit number on which the card number begins. Choose a starting value from 0 - 255.

Starting Bit for Issue Code

The bit number on which the issue code begins. Choose a starting value from 0 - 255.

Number of Bits in Facility Code

That portion of the total number of bits on the card that will be used for the facility code. Choose a value from 0 - 32 bits.

Number of Bits in Card Number

That portion of the total number of bits on the card that will be used for the card number. Choose a value from 0 - 64 bits.

Number of Bits in Issue Code

That portion of the total number of bits on the card that will be used for the issue code. Choose a value from 0 - 32 bits.

Number of Even Parity Bits

If parity is even, this field specifies the total value of parity bits in the Wiegand card format string. Choose a value from 0 - 256.

Number of Odd Parity Bits

If parity is odd, this field specifies the total value of parity bits in the Wiegand card format string. Choose a value from of 0 - 256.

Special

If you are using special card format features, select a special feature from this drop-down. Choices include:

None - Select if you are not using special card format features.

Step Parity Check by Two Bits - If selected, step parity is calculated by 2 bits

Four Parity Bit Check - If selected, enables 37-bit Parity Test with 4 Parity Bits

Middle Parity Check - If selected, enables 37-bit Parity Test with 2 Parity Bits in middle of the card.

HID Corporate 1000 - Select if you are using HID access panels. You are only allowed to save this format if the following conditions are satisfied:

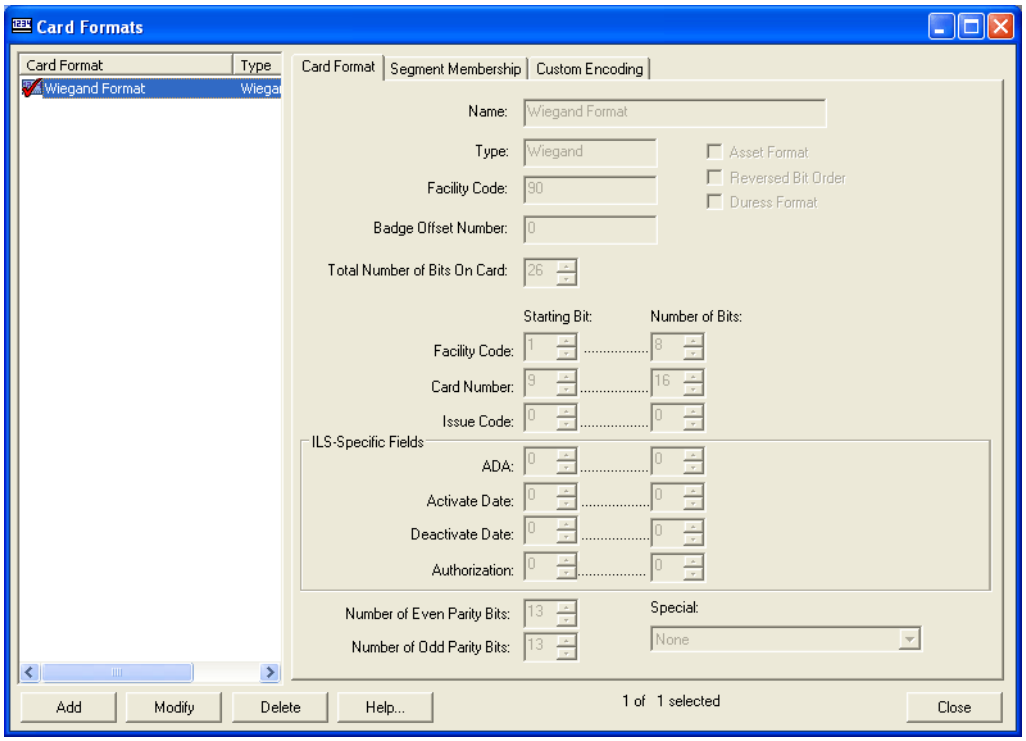
- "Total Number of Bits On Card" = 35
- "Facility Code" has a "Start Code" = 2
- "Facility Code" has a "Number of Bits" = 12
- "Card Number" has a "Start Code" = 14
- "Card Number" has a "Number of Bits" = 20
- "Issue Code" has a "Number of Bits" = 0

Notes: If the conditions are not met, you will be given the option of setting these conditions automatically.

Wiegand card formats configured with HID Corporate 1000 can only be referenced by HID Access Control (iCLASS) or (MIFARE) smart card formats.

GSA binary \ AC+SC+CC - If selected, it formats a 48-bit card number as follows: (bits 34 through 47)*(10**11)+(bits 20 through 33)*(10**7)+(bits 0 through 19).

Wiegand Card Format Form (ILS)



IMPORTANT: To view the ILS-specific fields on this form your system must have an ILS license.

Asset Format

When this box is checked, the selected card format can be configured for asset management.

The **Asset Format** check box should not be selected if the access levels associated with the badge has escort functionality.

Reversed Bit Order

(This option is supported only in series 2 Lenel access panels.) Identifies this card format as a reserved bit order format. When the controller detects this format, it reverses the bit order of the incoming data before processing it.

Readers report the duress state differently. For example, Bioscrypt readers report duress by reversing the bit order of the entire Wiegand string longitudinally. This setting is ignored during badge encoding.

Duress Format

(This option is supported only in series 2 Lenel access panels.) Identifies this card format as a reader duress card format. When the controller receives a duress format from the reader, it reports the access related events as duress followed by the access event description rather than normal standard reporting. For example: “DURESS - Access Grant” vs. “Access Grant”. This setting is ignored during badge encoding.

This setting is different than the **Deny On Duress PIN** setting for readers that accept PIN input. The deny on duress reader setting only functions using this setting and not the duress card format. For more information, refer to Settings Form on page 645.

Facility Code

Specifies a unique value for this facility. Choose a value less than 999999999.

Badge Offset Number

The **Badge Offset Number** field is utilized in the card format configuration to offset the badge number by the value entered in the field.

An example would be: If the actual card badge number is 1500 and the **Badge Offset Number** field is set to 1000 then the number reported in the access event would 2500. This is useful to keep duplicate badge ID's unique. When multiple independent systems are merged into one OnGuard system duplicate badge ID’s could become a problem. It is important that the access control hardware is able to uniquely identify the card format using the offset by a different facility code or card format structure.

If the Badge Offset Number is set to zero (0) then no offset is applied and the actual badge number is reported.

Choose a value less than 999999999.

Total Number of Bits On Card

The total number of bits encoded on the card with a maximum value of 256 bits.

The number of bits in **Facility Code**, **Issue Code**, **Card Number**, **ADA**, **Activate Date**, **Deactivate Date**, and **Authorization** combined must not exceed the total number of bits on the card. If one or more fields are out of range, the system will reset them to the maximum bits allowed.

Except for the parity bits, the fields should not overlap and the length of a field cannot extend beyond the length of the card.

Starting Bit for Facility Code
The bit number on which the facility code begins. Choose a starting value from 0 - 255.

Starting Bit for Card Number
The bit number on which the card number begins. Choose a starting value from 0 - 255.

Starting Bit for Issue Code
The bit number on which the issue code begins. Choose a starting value from 0 - 255.

Starting Bit for ADA
The bit number on which the ADA (Americans with Disabilities Act) information is stored. In order to be ADA-compliant, extended door time is assigned to cardholders with disabilities who require it. Choose a starting value from 0 - 255.

Starting Bit for Activate Date
The bit number on which the activate date begins. Choose a starting value from 0 - 222. Activate/deactivate time is stored as the number of seconds elapsed since midnight (00:00:00), January 1, 1970 to the specified time. The maximum date is January 18, 2038.

Starting Bit for Deactivate Date
The bit number on which the deactivate date begins. Choose a starting value from 0 - 222.

Starting Bit for Authorization
The bit number on which the authorization information begins. Choose a starting value from 0 - 215.

Number of Bits in Facility Code
That portion of the total number of bits on the card that will be used for the facility code. Choose a value from 0 - 32 bits.

Number of Bits in Card Number
That portion of the total number of bits on the card that will be used for the card number. Choose a value from 0 - 64 bits.

Number of Bits in Issue Code
That portion of the total number of bits on the card that will be used for the issue code. Choose a value from 0 - 32 bits.

Number of Bits in ADA
That portion of the total number of bits on the card that will be used for the ADA information. Choose a value of 0 or 1 bit.

Number of Bits in Activate Date
That portion of the total number of bits on the card that will be used for the activate date. Choose a value of either 0 or 32 bits.

Number of Bits in Deactivate Date
That portion of the total number of bits on the card that will be used for the deactivate date. Choose a value of either 0 or 32 bits.

Number of Bits in Authorization
That portion of the total number of bits on the card that will be used for the authorization information. Choose a value of either 0 or 40 bits.

Number of Even Parity Bits

If parity is even, this field specifies the total value of parity bits in the Wiegand card format string. Choose a value from 0 - 256.

Number of Odd Parity Bits

If parity is odd, this field specifies the total value of parity bits in the Wiegand card format string. Choose a value from of 0 - 256.

Special

If you are using special card format features, select a special feature from this drop-down. Choices include:

None - Select if you are not using special card format features.

Step Parity Check by Two Bits - If selected, step parity is calculated by 2 bits

Four Parity Bit Check - If selected, enables 37-bit Parity Test with 4 Parity Bits

Middle Parity Check - If selected, enables 37-bit Parity Test with 2 Parity Bits in middle of the card.

HID Corporate 1000 - Select if you are using HID access panels. You are only allowed to save this format if the following conditions are satisfied:

- "Total Number of Bits On Card" = 35
- "Facility Code" has a "Start Code" = 2
- "Facility Code" has a "Number of Bits" = 12
- "Card Number" has a "Start Code" = 14
- "Card Number" has a "Number of Bits" = 20
- "Issue Code" has a "Number of Bits" = 0

Notes: If the conditions are not met, you will be given the option of setting these conditions automatically.

Wiegand card formats configured with HID Corporate 1000 can only be referenced by HID Access Control (iCLASS) or (MIFARE) smart card formats.

GSA binary \ AC+SC+CC - If selected, it formats a 48-bit card number as follows: (bits 34 through 47)*(10**11)+(bits 20 through 33)*(10**7)+(bits 0 through 19).

Add a Wiegand Card Format

Your system can support a maximum of eight Wiegand card formats. This is a limitation of existing hardware. For ILS locking systems, a maximum of four Wiegand card formats are supported.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select "Wiegand" and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. If you want cards with this format to be available for asset assignment, select the **Asset Format** check box.

7. If you want cards with this format to be duress cards:
   a. If your reader reports duress by reversing the bit order, select the **Reversed Bit Order** check box.
   b. Select the **Duress Format** check box.
8. Enter the facility code for this format, if there is one.
9. If your system uses multiple card technologies with overlapping card numbers, specify an offset in the **Badge Offset Number** field.
10. Enter the total number of bits on the card. This information is available from the card vendor, and is usually a Wiegand standard number.
11. Enter the number of the Wiegand bit on which the facility code begins. Do the same for the card number and the issue code.
12. Enter the number of bits used for the card number, the facility code, and the issue code.
13. (Optional) Enter the number of bits used for the ADA information, the activate date, the deactivate date, and the authorization information.
14. (Optional) Enter the number of the Wiegand bit on which the ADA information begins. Do the same for the activate date, the deactivate date, and the authorization information.
15. If you are using special card format features, select a special feature from the **Special** drop-down.
16. Click [OK].

Standard 26-Bit Wiegand Card Formats

The following table suggests the settings to use for a standard 26-bit Wiegand card. Your organization may use a proprietary format instead. If so, your Wiegand card vendor can provide the configuration information required for the Card Format form.

Wiegand Card Format form Field Name	Value to Enter
Format Name	Wiegand (26)
Facility Code	0 (or other - see Determine the Facility Code on page 259.)
Total Number of Bits on Card	26
Badge Offset Number	(default is 0 - see the definition in Wiegand Card Format Form on page 252.)
Number of Bits in Card Number	16
Number of Bits in Facility Code	8
Number of Bits in Issue Code	0
Number of Even Parity Bits	13
Number of Odd Parity Bits	13
Starting Bit for Each Wiegand Field - Facility Code	1
Starting Bit for Each Wiegand Field - Card Number	9

Wiegand Card Format form Field Name	Value to Enter
Starting Bit for Each Wiegand Field - Issue Code	1

Determine the Facility Code

Your Wiegand card vendor provides the facility code. If you do not know your facility code, do the following:

1. Complete the Wiegand Card Format form as described in Standard 26-Bit Wiegand Card Formats on page 258 or Standard 75-Bit PIV Card Formats on page 259.
2. Continue configuring the rest of your system.
3. Swipe a valid badge through a card reader on your system. This will trigger an Invalid Facility Code event. In the Alarm Monitoring application, the event will indicate the correct facility code in the Main Alarm Monitor window.
4. You can then return to the Wiegand Card Format form and modify it to specify the correct facility code.

Your Wiegand card vendor also provides card numbers. In the **Generate Badge ID** field (located on the Badge ID Allocation form in the Cardholder Options folder), choose one of the following fields:

Automatic if your vendor has given you sequential Wiegand card numbers. Be sure also to enter an accurate **Badge Offset Number** value on the Wiegand Card Format form.

Manual Entry if your Wiegand card numbers are not sequential. This means that you will have to enter each **Badge ID** (card number) manually when adding badges using the Badge form in the Cardholders folder.

Standard 75-Bit PIV Card Formats

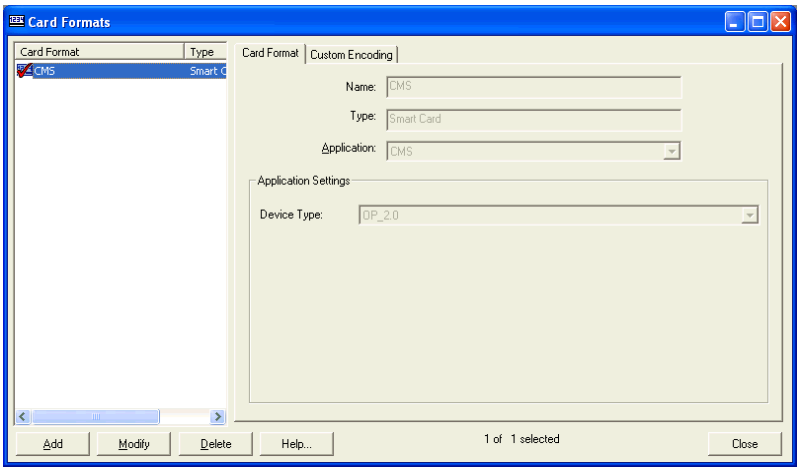
The following table suggests the settings to use for a standard 75-bit PIV card. Your organization may use a proprietary format instead. If so, your Wiegand card vendor can provide the configuration information required for the Card Format form.

PIV Card Format form Field Name	Value to Enter
Format Name	PIV (75)
Facility Code	0 (or other - see Determine the Facility Code on page 259.)
Total Number of Bits on Card	75
Badge Offset Number	(default is 0 - see the definition in Wiegand Card Format Form on page 252.)
Number of Bits in Card Number	48
Number of Bits in Facility Code	0
Number of Bits in Issue Code	0
Number of Even Parity Bits	38

PIV Card Format form Field Name	Value to Enter
Number of Odd Parity Bits	37
Starting Bit for Each Wiegand Field - Facility Code	0
Starting Bit for Each Wiegand Field - Card Number	1
Starting Bit for Each Wiegand Field - Issue Code	0
Special	GSA binary PIV AC+SC+CC

CMS Card Format Form

This view displays when “CMS” is selected from the **Application** drop-down.



Device Type

Identifies the CMS Device Type by its name. Currently ActivIdentity CMS only supports the “OP_2.0” device type.

CMS listing window

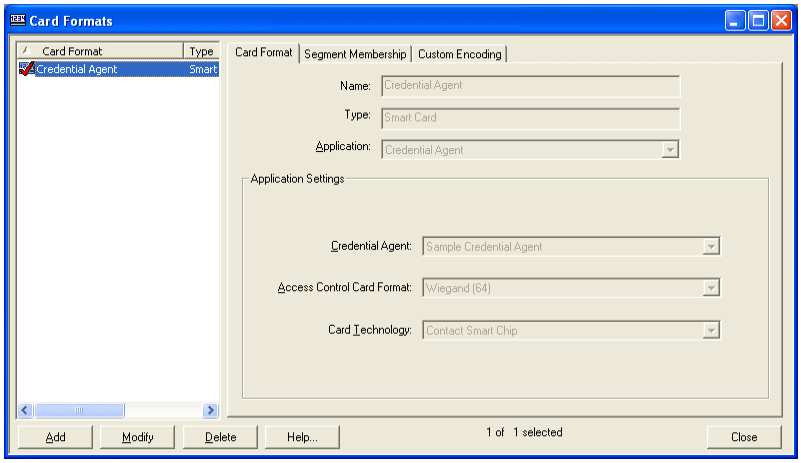
Displays the name, hostname, and port of CMS systems configured for use with the OnGuard system.

CMS Card Format Form Procedures

For instructions on how to configure and use CMS, refer to Appendix I: Integrating ActivIdentity CMS with OnGuard on page 1453.. The following procedure in that section is performed in this folder: Add a CMS Smart Card Format on page 1459.

Credential Agent Card Format Form

This view displays when “Credential Agent” is selected from the **Application** drop-down.



Note: Credential Agent applications do not require special licensing.

Credential Agent

The name of the third party application registered with OnGuard that will be called during encoding. The Credential Agent field automatically populates with “Sample Credential Agent”, which demonstrates the features of the Credential Agent card format. Use the sample (COM application) to write your own credential agent.

Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

Card Technology

Identifies the type of card this card format is associated with.

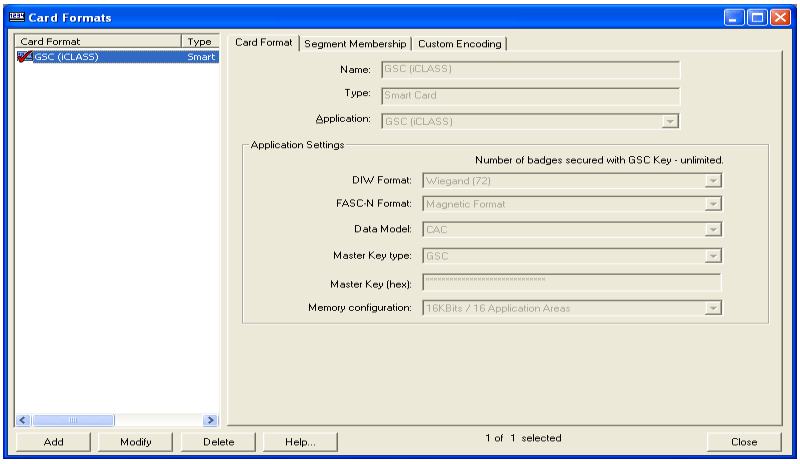
Add a Credential Agent Smart Card Format

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select **Credential Agent** from the **Application** drop-down.
7. In the **Credential Agent** field, select the third party application registered with OnGuard that will be called during encoding.

8. Select the previously configured Wiegand access control card format from the **Access Control Card Format** drop-down. Any Wiegand card format with standard settings is acceptable. Special Wiegand card format settings are not required for Credential Agent applications.
9. Verify the correct card technology is selected. If not, select the card technology you want associated with this card format, from the drop-down.
10. Click [OK].

GSC (iCLASS) Card Format Form

This view displays when “GSC (iCLASS)” is selected from the **Application** drop-down.



Note: GSC (iCLASS) applications do not require special licensing.

Number of badges secured with GSC Key

Displays the number of badges that are able to be secured with a GSC Key. If you are using GSC Key for encoding, you can encode unlimited cards, but if you are using custom key, the number is determined by your license.

DIW Format

A custom Wiegand format. The Device Independent Wiegand (DIW) format must be created before you configure a government smart card format. The DIW format can be up to 128 bits in length.

Refer to Wiegand Card Format Configurations for GSC (iCLASS) Applications (Default Settings) on page 264 for the default DIW settings.

Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

FASC-N Format

A customized magnetic card format. A Federal Agency Smart Credential Number (FASC-N) magnetic card format must be created before you configure a government smart card format. All magnetic card formats configured in the system are available from the drop-down.

Data Model

The data model used to map data. Only user-defined fields that are mapped to a selected data model will be stored on a card. Fields are mapped to data models in FormsDesigner.

Master Key type

The type of key preprogrammed on smart card readers. Choices include: Custom and GSC. If you choose Custom you must also fill in the **Master Key (hex)** field with a series of 16 hexadecimal digits. If you choose GSC the **Master Key (hex)** field is populated automatically.

Master Key (hex)

A hex value preprogrammed on smart card readers that protects Federal Agency Smart Credential Number (FASC-N) and demographic data. This field automatically populates when you select the master key type GSC.

Memory configuration

The memory configuration of the smart card readers. The default memory configuration is 16K Bits/16 Application Areas which provides the greatest compatibility with different readers. Choices include:

- 16kbits/16 Application Areas
- 16kbits/2 Application Areas (Custom Key)
- 16kbits/16 Application Areas (Custom Key)

Add a GSC (iCLASS) Smart Card Format

Note: GSC (iCLASS) applications require a custom Wiegand (DIW) format where the total number of bits on a card does not exceed 128.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select “GSC (iCLASS)” from the **Application** drop-down.
7. Select the DIW and FASC-N format.
8. Verify the data model format is correct. If not, use the **Data Model** drop-down to select the correct format.
9. The **Master Key Type** and **Master Key (hex)** fields automatically populate. If you wish to add a custom master key do the following:
   a. To use a custom master key you must first have a license (SWG-1490).
   b. Choose “Custom” from the **Master Key Type** drop-down field.
   c. Type the key you wish to use in the **Master Key (hex)** field.

Note: Once cards are secured using a custom key, data imports from GSC (iCLASS) cards will be disabled.

10. Verify the memory configuration value is correct. If not, use the drop-down to select the correct configuration.

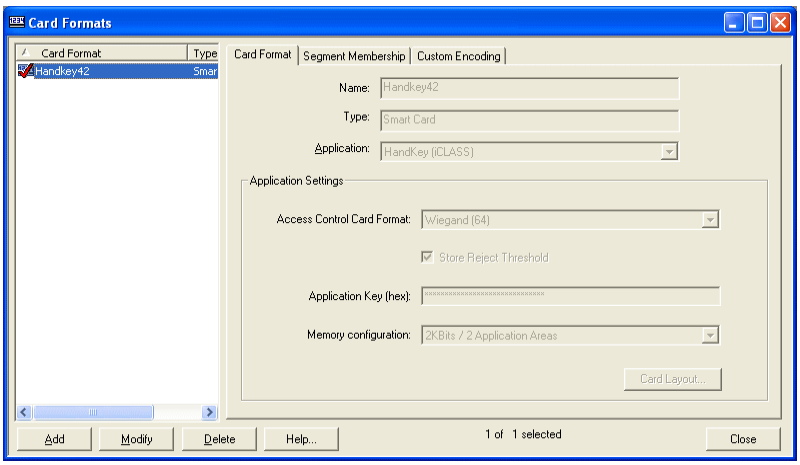
11. Click [OK].

Wiegand Card Format Configurations for GSC (iCLASS) Applications (Default Settings)

Field name	Configuration
Name	DIW
Type	Wiegand
Facility Code	User configurable
Badge Offset Number	User configurable
Total Number of Bits on Card	64
Facility Code/Starting Bit	0
Facility Code/Number of Bits	8
Card Number/Starting Bit	8
Card Number/Number of Bits	48
Issue Code/Starting Bit	56
Issue Code/Number of Bits	8
Number of Even Parity Bits	0
Number of Odd Parity Bits	0
Special	None

HandKey (iCLASS) Card Format Form

This view displays when “HandKey (iCLASS)” is selected from the **Application** drop-down.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. Wiegand card formats configured with HID Corporate 1000 can only be referenced by HID Access Control (iCLASS) smart card formats.

Store Reject Threshold

If checked, the card stores the reject threshold that was determined in the HandKey hand geometry template in the Multimedia Capture module.

Application Key (hex)

A key used to authenticate and secure application areas containing the biometric container on the smart card. The default application key is “Default HID Kd for Page 0 App 1”. The HandKey Access system must be configured to use the same application key in order to gain access to application areas holding the biometric container with HandKey handprint data.

The application key must be 16 hexadecimal digits long. Only hex digits (1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, and A, B, C, D, E, F) are allowed.

This is a secure field. The application key is only visible when you enter the key value. After the key is stored, it displays as a predefined number of “*”.

Memory configuration

The memory configuration of the smart card readers. The default memory configuration is 16K Bits/16 Application Areas which provides the greatest compatibility with different readers.

Card Layout

The card layout is populated with a default configuration, and you should not modify the card layout unless you are very familiar with iCLASS card memory layout. However, if you desire to change the configuration, the following guidelines should be followed:

- Default layout configuration for memory configuration of 16K/16 Application areas: Page 0 /Application 2 is used for Application data. All other Applications are unused.
- Default layout configuration for memory configuration of 16K/2 Application areas or 2K/2 Application areas: Application data starting offset is 0x0013. Location of application data must also be Page 0/Application 2.

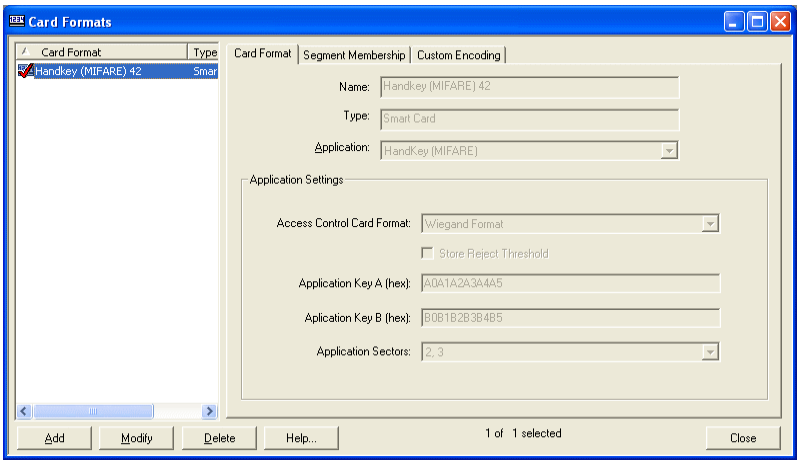
Add a HandKey (iCLASS) Card Format

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select “HandKey (iCLASS)” from the **Application** drop-down.
7. Select the previously configured Wiegand access control card format from the **Access Control Card Format** drop-down. Any Wiegand card format with standard settings is acceptable. Special Wiegand card format settings are not required for Credential Agent applications.
8. Enter the 32 character hex value for the application key.

9. Select the memory configuration you wish to use.
10. Click [OK].

HandKey (MIFARE) Card Format Form

This view displays when “HandKey (MIFARE)” is selected from the **Application** drop-down.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding.

Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

Store Reject Threshold

If checked, the card stores the reject threshold that was determined in the HandKey hand geometry template in the Multimedia Capture module.

Application Key A (hex)

A public key used for authentication to read sectors on a MIFARE card. Key A automatically populates with the default (secret) key.

If you are using the native Integrated Engineering tools to configure readers and you change key A, make sure that the reader parameter, KEYASA, matches what ever you enter in this field. If you are using the stand alone utility to configure readers, make sure the settings in the IEConfiguration Card Utility match what ever you enter in this field.

Key A must be a 6 byte hex value. Therefore, the value must be 12 characters long and contain numbers 0-9 and/or letters A-F.

Application Key B (hex)

A covert key used for authentication to secure a MIFARE card. Key B protects the sector that holds access control data. By default, this key is set to a secret key.

New (blank) MIFARE cards - have a transport configuration protected by default keys. Any number you enter in the **Key B** field overwrites the transport configuration. Note that key B must be a hex value.

Old (used) MIFARE cards - have information already written on them and are no longer in transport configuration. You must enter the current key in order to encode the card.

Application Sectors

Choose the application sectors that match what is expected by the reader. This configuration is determined by the System Administrator. The default sectors are 2 and 3.

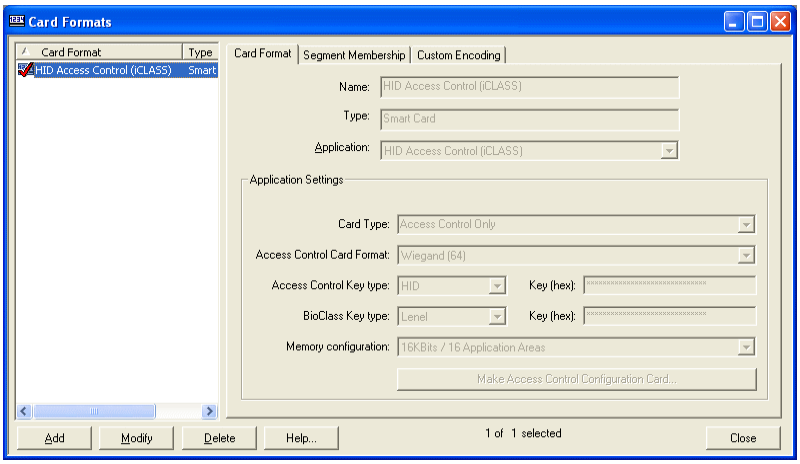
Add a HandKey (MIFARE) Card Format

Note: When assigning a HandKey (MIFARE) card format to a badge the cardholder's badge ID must be less than or equal to the value 65535.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select "Smart Card" and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select "HandKey (MIFARE)" from the **Application** drop-down.
7. Select the previously configured Wiegand access control card format from the **Access Control Card Format** drop-down. Only standard Wiegand 26-bit card format is acceptable.
8. If you want to customize the application keys, enter application key A and B. If you are working with a previously used card, you must enter the previously configured key B. Otherwise, use the application key default values.
9. Choose the application sectors you wish to use.
10. Click [OK].

HID Access Control (iCLASS) Card Format Form

This view displays when "HID Access Control (iCLASS)" is selected from the **Application** drop-down.



Card Type

The card type sets what information you want encoded onto the card. Choice include:

- **Access Control Only** - Choose if you want to create an access control smart card.
- **Access Control With BioClass** - Choose if you want to create a card with both access control and BioClass features.
- **Add BioClass** - Choose if you want to add BioClass data to an existing access control smart card.

Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. The maximum length of the access control data encoded in the HID applications area of iCLASS cards is 143 bits. This accommodates the sentinel bit required by HID readers.

Access Control Key type

The type of key preprogrammed on smart card readers. Choices include: Lenel, HID, and Custom. If you choose Custom you must also fill in the **Master Key (hex)** field with a series of 16 hexadecimal digits. If you choose HID or Lenel the **Master Key (hex)** field is populated automatically. For more information, refer to the Make Configuration Card definition in this table. You can not make a configuration card and use a Custom key type

Key (hex)

A hex value of the Lenel Security Master key that is preprogrammed on smart card readers and protects access control data. This field automatically populates when you select the HID or Lenel Access Control Key type.

BioClass Key Type

The type of key preprogrammed on smart card readers. Choices include:

- **Lenel** - Uses the default Lenel bioCLASS key. In this case, the Lenel bioCLASS key is used to secure the data on the (iCLASS) smart card
- **Custom** - Choosing Custom allows the operator to manually enter in a custom key. In this case, the custom key entered here by the operator is used to secure the data on the (iCLASS) smart card. Custom keys are a licensed feature.

For more information, refer to the Make Configuration Card definition in this table.

You can not make a configuration card and use a Custom key type

Key (hex)

A hex value of the Lenel Security Master key that is preprogrammed on smart card readers and protects access control data. This field automatically populates when you select the Lenel BioClass Key type.

Memory configuration

The memory configuration of the smart card readers. The default memory configuration is 16K Bits/16 Application Areas which provides the greatest compatibility with different readers.

Make Access Control Configuration Card

Click this button to select the encoder to create a configuration card. Clicking this button opens the Encoder Listing window. Here you must choose the:

- **Configuration Type** - The configuration type that you choose is based on which key type (BioClass or Access Control) you are using on the Card Formats form.
- **Encoder** - Choose the encoder that you want to use from the drop-down box.

Configuration cards are used to configure keys in HID Access Control (iCLASS) card format readers and to set default parameters.

Using configuration cards, you can change the master key of the reader from HID to Lenel or set default Lenel settings on the reader. The type of configuration card that you create is based on the master key type. Select Lenel as the master key type, to make a configuration card that will change the master key from HID to Lenel. Select HID as the master key type to change the default parameters in the reader.

Application License - HID Access Control (iCLASS)

The iCLASS Access Control Support (STD) license is required to use the HID Access Control (iCLASS) application.

Add an HID Access Control (iCLASS) Smart Card Format

Note: HID Access Control (iCLASS) applications require a Wiegand format where the total number of bits on a card does not exceed 143.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. From the list, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment to which this card format will be assigned.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select “HID Access Control (iCLASS)” from the drop-down.
7. Select a card type from the **Card Type** drop-down box.
8. Select the previously configured Wiegand access control card format you want this smart card to reference from the **Access Control Card Format** drop-down.
9. Depending on the card you are creating choose from the **Access Control Key type** and **BioClass Key type** drop-down boxes.

Note: The corresponding **Key (hex)** fields automatically populate depending on your choices.

10. Verify the memory configuration value is correct. If not, use the drop-down to select the correct configuration.
11. Click [OK].

Create an HID Access Control (iCLASS) Reader Configuration Card

Configuration cards can be created using native iCLASS tools or by using a stand alone utility. The following procedure creates a configuration card for various iCLASS readers using an iCLASS encoder and native iCLASS tools.

To use the stand alone HID iCLASS Utility, refer to the Supplemental Materials disc.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Select (place a checkmark beside) the HID Access Control (iCLASS) card format.
3. Verify the Application Settings are correct. To change the master key from HID to Lenel, select "Lenel" on the **Access Control Key type** field. To set default parameters, select "HID" instead. The **BioClass Key type** field must be set to "Custom".

Notes: You can create a configuration card to change the master key of an HID Access Control (iClass) reader from HID to Lenel, or to set default Lenel settings on the reader.

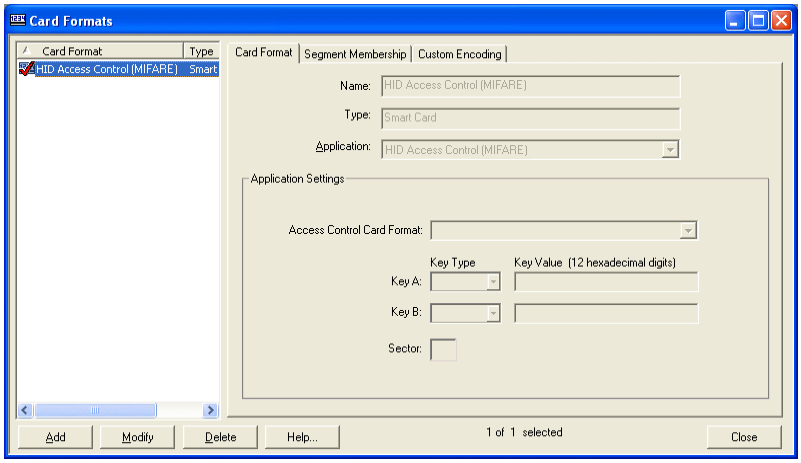
The decision on which card to create (HID or Lenel) is based on the **Access Control Key type** field. If you select "HID" the following default parameters will be set in the reader:

- Beep will be on
- LED will normally be red
- Reader will flash green on tag read

4. Click [Make Access Control Configuration Card].
5. The Encoder Listing window opens. Select the configuration type and encoder from the drop-down.
6. Click [OK].
7. Follow any prompts that display to encode the configuration card.

HID Access Control (MIFARE) Card Format Form

This view displays when "HID Access Control (MIFARE)" is selected from the **Application** drop-down.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding.

The maximum length of the access control data encoded in the HID applications area of MIFARE cards is 119 bits. This accommodates the sentinel bit required by HID readers.

Key type

The type of key preprogrammed on smart card readers. Choices include: Custom and HID. If you choose Custom you must also fill in the **Key Value** field with a series of 12 hexadecimal digits. If you choose HID the **Key Value** field is populated automatically.

Key Value (12 hexadecimal digits)

When creating a custom key type, enter 12 hexadecimal digits into this field. The only characters allowed are a-f, A-F, and 0-9.

Sector

Use this field to select which sector to use. This must match what is expected by the reader. This configuration is determined by the System Administrator. The sector is 2 digits long.

Application License - HID Access Control (MIFARE)

The HID Access Control (MIFARE) license is required to use the HID Access Control (MIFARE) application.

Add an HID Access Control (MIFARE) Smart Card Format

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select a “HID Access Control (MIFARE)” from the drop-down.

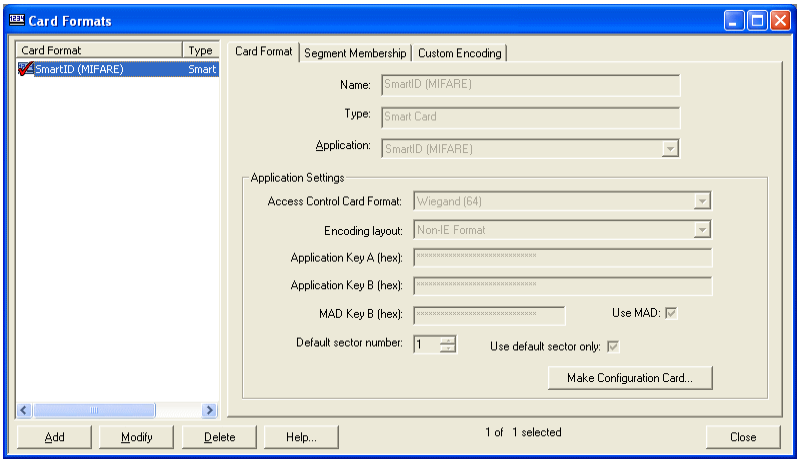
7. Select the previously configured Wiegand access control card format you want this smart card to reference from the **Access Control Card Format** drop-down.
8. Choose a key type in the Key A and Key B section of the screen. Select HID to populate the **Key Value** field automatically. Select **Custom** if you want to fill in the key value yourself.
9. In the Sector field, enter the 2 digit sector that the reader has been configured for. This is configured by the System Administrator.
10. Click [OK].

Create an HID Access Control (MIFARE) Reader Configuration Card

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Select (place a check mark beside) the HID Access Control (MIFARE) card format.
3. Verify the Application Settings are correct. To change the master key from HID to Lenel, select "Lenel" on the **Master Key type** field. To set default parameters, select "HID" on the **Master Key type** field.
4. Click [Make Configuration Card].
5. The Encoder Listing window opens. Select the encoder from the drop-down.
6. Click [OK].
7. Follow any prompts that display to encode the configuration card.

SmartID (MIFARE) Card Format Form

This view displays when "SmartID (MIFARE)" is selected from the **Application** drop-down.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

Encoding layout

Select the format the access control data should be encoded in. If you are using the native SmartID tools to configure readers and you select IE Format as the encoding layout, then the reader parameter must be configured to read IE Format (IEFORMAT=Y). If you select Non-IE Format as the encoding layout, then the reader parameter must be set to IEFORMAT=N.

The SmartID reader's output always contains parity. If you are encoding a card using IE format, the parity in the Wiegand format that is linked to the SmartID (MIFARE) application must match the reader's parity.

IE calculates parity for each half of the Wiegand data. So, if you have 18 bits of data, parity will be calculated over the first 9 and last 9 bits. If you have an odd number of bits, for example 21 bits, parity will be calculated over the first 11 and last 11 bits.

Application Key A (hex)

A public key used for authentication to read sectors on a MIFARE card. Key A automatically populates with the default (secret) key. If you are using the native Integrated Engineering tools to configure readers and you change key A, make sure that the reader parameter, KEYASA, matches what ever you enter in this field. If you are using the stand alone utility to configure readers, make sure the settings in the IEConfiguration Card Utility match what ever you enter in this field. Note that key A must be a 6 byte hex value. Therefore, the value must be 12 characters long and contain numbers 0-9 and/or letters A-F.

Application Key B (hex)

A covert key used for authentication to secure a MIFARE card. Key B protects the sector that holds access control data. By default, this key is set to a secret key. New (blank) MIFARE cards - have a transport configuration protected by default keys. Any number you enter in the **Key B** field overwrites the transport configuration. Note that key B must be a hex value. Old (used) MIFARE cards - have information already written on them and are no longer in transport configuration. You must enter the current key in order to encode the card.

Use MAD

This check box enables the MIFARE application directory (MAD) and writes MAD onto a MIFARE card. If you enable MAD, sector zero stores the application ID that tells the reader what sector to read. When you enable MAD, a new entry is made into the card, if MAD exists on the card. If MAD does not exist, MAD will be created and a new entry made into the card. If you do not enable MAD, the application will be written into the sector specified by the user in the **Default Sector Number** text box.

MAD Key B (hex)

A covert key for authentication to write to the MIFARE application directory (if MAD is enabled). MAD key B is a 32 character hex value. *Hex values* contain numbers 0-9 and/or letters A-F. By default, this key is set to a secret key. If MAD already exists on the card, then the current MAD key B should be entered. If the user is not an owner of MAD, then the user must find out what the current key is before MAD can be written. Once MAD is created, MAD key B will be used if other applications are programmed on to the card. MAD key B should only be released to people who will write other applications.

Default sector number

The sector number the IE application is written to. The default sector number cannot be zero because MAD uses/reserves this sector. The default sector is read with key A and secured with key B. If authentication cannot be performed and MAD is on the card, then the application will search MAD for the next available sector to write the IE application to.

Use default sector only

Specifies the course of action if the specified (default) sector is not available. This check box is automatically enabled if the **Use MAD** check box is not selected.

- If MAD is available and the **Use default sector only** check box is selected, then the specified sector number is used. If this sector cannot be overwritten, the application returns an error.
- If MAD is available and the **Use default sector only** check box is not selected, then the first sector available on the card will be used to encode the IE application if the specified sector isn't available. If no sector is available an error will be returned.
- If MAD is not used then the **Use default sector only** check box is automatically enabled and the application will be written into the sector specified by the user.

Make Configuration Card

Click this button to select the encoder to create a configuration card. Configuration cards are used to configure keys in SmartID (MIFARE) card format readers and to set default parameters.

Application License - SmartID (MIFARE)

A license (SWG-1402) is required to use the SmartID (MIFARE) application.

Add a SmartID (MIFARE) Smart Card Format

IMPORTANT: SmartID (MIFARE) applications require a Wiegand format where the total number of bits on a card does not exceed 128 for Non-IE formats and 64 for IE formats.
Furthermore, the value you enter in the **Total Number of Bits On Card** field must also be entered as the CARDLEN parameter for the configuration card. For more information on using the configuration card to configure readers, refer to the Hardware Installation Guide.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select "Smart Card" and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select a "SmartID (MIFARE)" from the drop-down.
7. Select the previously configured Wiegand access control card format you want this smart card to reference from the **Access Control Card Format** drop-down.
8. Select the encoding layout.
9. If you want to customize the application keys, enter application key A and B. If you are working with a previously used card, you must enter the previously configured key B. Otherwise, use the application key default values.
10. Select the **Use MAD** check box if you want to write MAD onto the MIFARE card.
11. If you selected the **Use MAD** check box and if MAD already exists on the card, then enter the current MAD key B. Otherwise, use the MAD key B default value.
12. Enter the default sector number regardless of whether you are using MAD or not.
13. If you are using MAD and only want to write to the default sector, verify the **Use Default Only** check box is selected.
14. Click [OK].

Create a SmartID (MIFARE) Reader Configuration Card

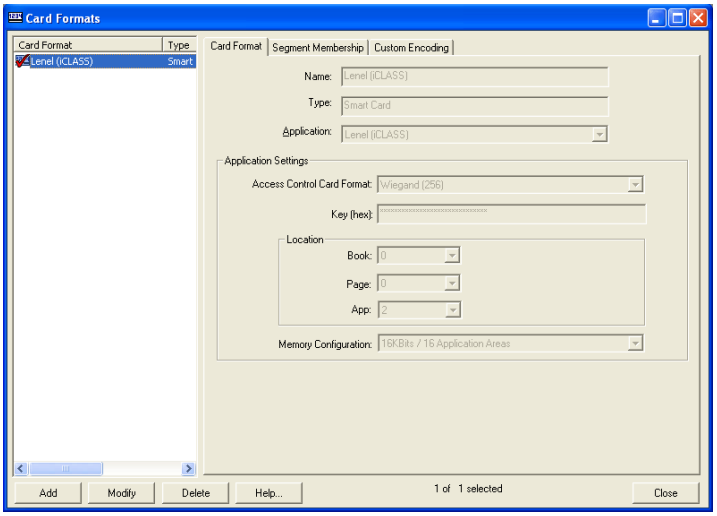
Configuration cards can be created using native Integrated Engineering tools or by using a stand alone utility. The following procedure creates a configuration card for IE PX007 (MIFARE) readers using the GemEasyLink680S/GemEasyAccess332 encoder and native Integrated Engineering tools.

For more information on using the stand alone IEConfiguration Card Utility, refer to the MIFARE Readers chapter in the Alternative Reader Wiring Guide.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Select (place a checkmark beside) the SmartID (MIFARE) card format.
3. Verify the Application Settings are correct.
4. Click [Make Configuration Card].
5. The Encoder Listing window opens. Select the GemEasyLink680S/GemEasyAccess332 encoder from the drop-down.
6. Click [OK].
7. Follow any prompts that display to encode the configuration card.

Lenel (iCLASS) Card Format Form

This view displays when “Lenel (iCLASS)” is selected from the **Application** drop-down.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

Key (hex)

The key that is used to access the application area of the card. The value must be 16 hexidecimal digits long and contain the numbers 0-9 and/or the letters A-F.

This is a secure field. The application key is only visible when you enter the key value. After the key is stored, it displays as a predefined number of “*”.

Location

Specifies where the Lenel (iCLASS) application is stored in terms of Book, Page, and Application.

- **Book** - Select a value of 0 or 1.
- **Page** - Select a value from 0 - 7.
- **App** - Select a value of 1 or 2.

The default value is Book 0, Page 0, App 2. Book 0, Page 0, App 1 is reserved for the HID Access Control (iCLASS) application. You must select a different location for the Lenel (iCLASS) application.

For Book 1, 32K iCLASS cards are required to encode the ILS data using an HID (iCLASS) PROG encoder Rev.B. For more information, refer to Configure ILS iCLASS Printing and Encoding on page 1513.

Specify the memory configuration that is applied to the Book Location.Choices include:

- 16KBits/16Application Areas
- 16KBits/16Application Areas (Inside)
- 16KBits/2Application Areas
- 16KBits/2Application Areas (Inside)
- 2KBits/2Application Areas
- 2KBits/2Application Areas (Inside)

The default value is 16KBits /16Application Areas. For Book 1, select 16KBits/2Application Areas (Inside) or 16KBits/16Application Areas (Inside), only.

For Page values greater than zero (0), select 16KBits/16Application Areas or 16KBits/16Application Areas (Inside), only.

Add a Lenel (iCLASS) Smart Card Format

Note: Lenel (iCLASS) applications require a Wiegand format where the total number of bits on a card does not exceed 256.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. From the list, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment to which this card format will be assigned.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select a “Lenel (iCLASS)” from the drop-down.
7. Select the Wiegand access control card format you want this smart card to reference from the **Access Control Card Format** drop-down.

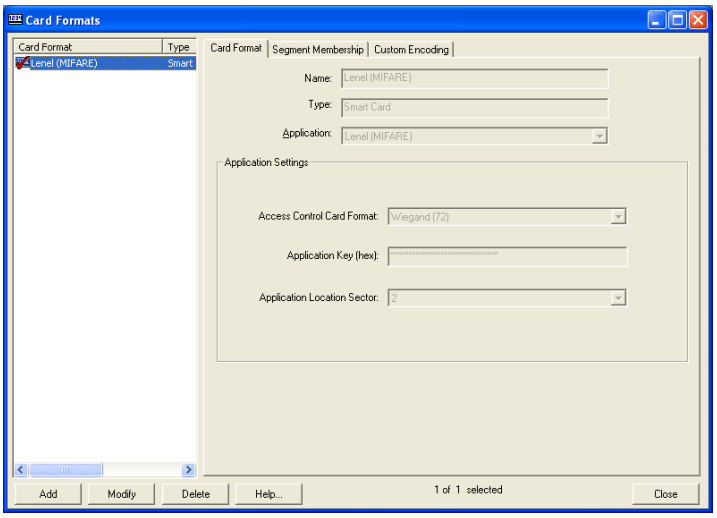
Note: Be sure to select a Wiegand card format configured with standard parity. Do not choose a Wiegand card format configured with HID Corporate 1000.

8. Enter a hex key.
9. Verify the memory configuration value is correct. If not, use the drop-down to select the correct configuration.
10. Click [OK].

Lenel (MIFARE) Card Format Form

(Depending on your version of OnGuard, this option may not be available.)

This view displays when “Lenel (MIFARE)” is selected from the **Application** drop-down.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

Application Key (hex)

A key used to authenticate to and secure the sectors containing the Lenel (MIFARE) application data. The application key authenticates to all data blocks in the sector identified in the **Application Location Sector**. This key is a 6-byte hex value. Therefore, the value must be 12 characters long and contain numbers 0-9 and/or letters A-F.

This is a secure field. The application key is only visible when you enter the key value. After the key is stored, it displays as a predefined number of “*”.

Application Location Sector

Specifies where the Lenel (MIFARE) application is stored in terms of sector. By default, the ILS (MIFARE) application is stored in sector 2, and occupies blocks 0, 1, and 2 (48 bytes).

The following application locations are supported:

- MIFARE Classic 1 K card: sector 0 - 15
- MIFARE Classic 4 K card: sector 0 - 32

If 16 - 32 is specified for the **Application Location Sector**, and a MIFARE Classic 1 K card is presented, the Invalid Smart Card Location event will be generated.

Add a Lenel (MIFARE) Smart Card Format

(Depending on your version of OnGuard, this option may not be available.)

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select “Smart Card” and click [OK].

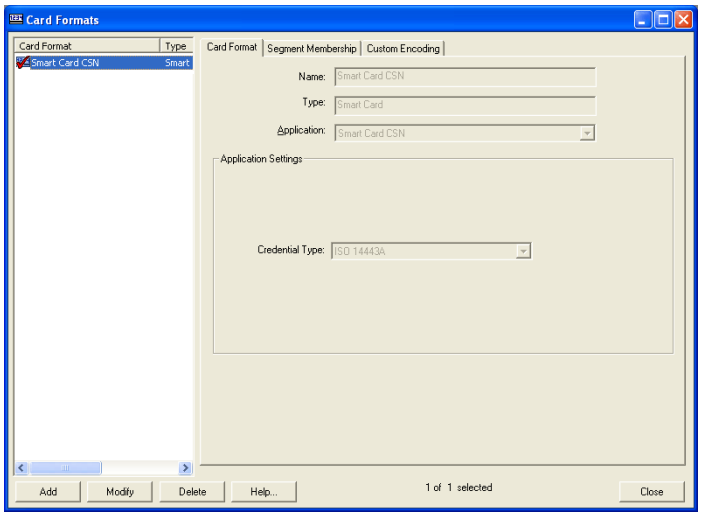
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select a “Lenel (MIFARE)” from the drop-down.
7. Select the previously configured Wiegand access control card format you want this smart card to reference from the **Access Control Card Format** drop-down.

Note: Be sure to select a Wiegand card format configured with standard parity. Do not choose a Wiegand card format configured with HID Corporate 1000.

8. Enter the 12-character hex value for the application key.
9. Select the sector where the application is stored in the **Application Location Sector** field.
10. Click [OK].

Smart Card CSN Card Format

This view displays when “Smart Card CSN” is selected from the **Application** drop-down.



Credential Type

Lists the CSN (Card Serial Number) card format types used for credential identification. Each smart card contains a unique permanent identification number (UID). This UID is also referred to as the Card Serial Number (CSN). The reader uses a compatible credential method to access the access control data encoded on the card. ISO 14443 is the International standard for contactless, proximity technology allowing a read range distance up to 10 centimeters. ISO 14443A is the leading standard for access control and transportation. An alternative standard for contactless, vicinity technology is ISO 15693 that allows a read range up to 50 centimeters. The advantage of using ISO 14443A is faster transaction speed. Choices include:

- **ISO 14443A** - Specifies the retrieval of a 4 or 7-byte card serial number from the ISO 14443A credential in the proximity of the reader. This method of identification supports MIFARE and DESFire Cards. Application Location and Application Key are not utilized by this card format.

- **ISO 15693** - Specifies retrieval of an 8-byte card serial number from the ISO 15693 credential in the vicinity of the reader. This method of identification supports iCLASS and other ISO 15693 credentials.

Because HID iCLASS readers output the entire 64 bits of the CSN, when Badge ID is imported from iCLASS cards in OnGuard, the Badge ID is converted to match the HID output. Therefore, you must configure the Wiegand card format as follows:

- **Total Number of Bits On Card** is set to 64 bits.
- **Card Number Starting Bit** is set to 0.
- **Card Number Number of Bits** is set to 56.
- All other numeric fields are set to 0.

Not all ISO 15693 readers (such as those from third parties) output the entire 64 bits of the CSN, or use the same byte order. In such cases, Badge ID must be produced using alternative methods.

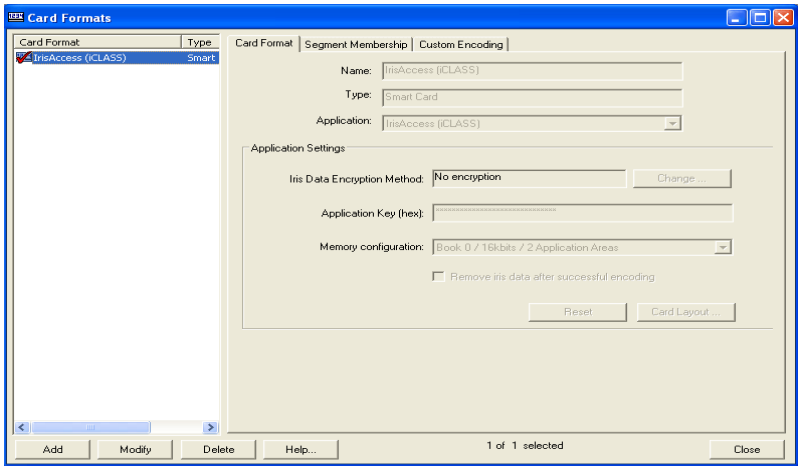
Add a Smart Card CSN Card Format

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. From the list, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment to which this card format will be assigned.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select a “Smart Card CSN” from the drop-down.
7. Select a **Credential Type** from the drop-down.
8. Click [OK].

IrisAccess (iCLASS) Card Format Form

This view displays when “IrisAccess (iCLASS)” is selected from the **Application** drop-down.

For more information about the IrisAccess system, refer to the Multimedia Capture appendix.



Notes: The IrisAccess (iCLASS) application is licensed by the number of cardholders who have their irises captured.

IrisAccess (iCLASS) must always be used in conjunction with the HID Access Control (iCLASS) Application encoded in the default location on Book 0.

Iris Data Encryption Method

Displays the data encryption method and type of respective data encryption key (not to be confused with Application Key). The selected encryption method will be applied to iris data prior to storing it to the smart card. The IrisAccess system must be configured to apply the same method in order to gain access to iris data after extracting it from the biometric container stored on the smart card.

This field does not affect the encryption method used for storing iris data in the OnGuard database.

Change

Displays the Key Management window where you can modify the data encryption method and/or generate a new key. For more information, refer to Key Management Window on page 281.

Application Key (hex)

A key used to authenticate and secure application areas containing the biometric container on the smart card. The default application key is “Default HID Kd for Page 0 App 1”. The application key must be 16 hexadecimal digits long. Only hex digits (1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, and A, B, C, D, E, F) are allowed.

This is a secure field. The application key is only visible when you enter the key value. After the key is stored, it displays as a predefined number of “*”.

The IrisAccess system must be configured to use the proper application key in order to gain access to application areas holding the biometric container with IrisAccess data. When encoding with the IrisAccess iCAM, this application key in OnGuard is not used. Instead, the application key should be configured using the IrisAccess iCAM web page.

Memory configuration

The following memory configurations can be selected:

- Book 0/16kbits/2 Application Areas
- Book 0/16kbits/16 Application Areas
- Book 0/16kbits/2 Application Areas (Custom Key)
- Book 0/16kbits/16 Application Areas (Custom Key)
- Book 1/16kbits/2 Application Areas (Custom Key)
- Book 1/16kbits/16 Application Areas (Custom Key)

The default memory configuration is Book 0/16kbits/2 Application Areas. This configuration assures faster access to the biometric container. When Book 1/16kbits/16 Application Areas or Book 1/16kbits/2 Application Areas is selected, the IrisAccess application will be written to Book 1 according to the selected card layout. Book 0 remains untouched. If Book 0 is selected, Book 1 remains untouched.

When you encode to Book 1, 32K iCLASS cards are required.

Remove iris data after successful encoding

Selecting this check box deletes the biometric data after it has been captured and encoded. This clears the data from the system for security purposes.

Reset

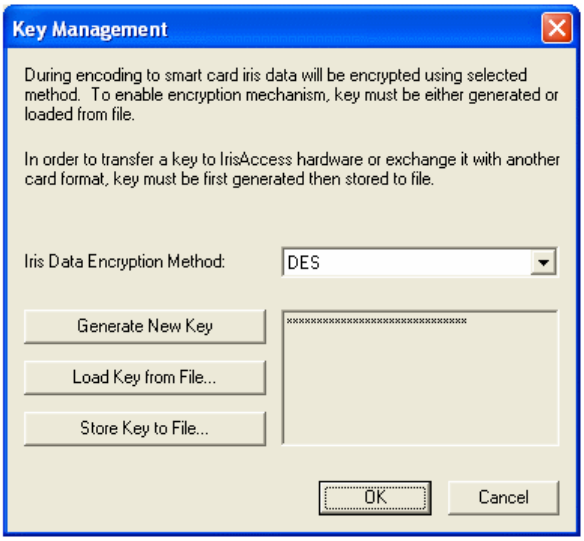
By pressing the [Reset] button, application settings will reset to their default values.

Card Layout

The card layout is populated with a default configuration, and you should not modify the card layout unless you are very familiar with iCLASS card memory layout.

- Default layout configuration for memory configuration of 16K/16 Application areas: Page 0/ Application 2, Page 1/Application 1, Page 2/Application 1, Page 3/Application 1, Page 4/ Application 1, Page 5/Application 1 are used for Application data. All other Applications are unused.
- Default layout configuration for memory configuration of 16K/2 Application areas: Application data starting offset is 0x0013. Location of application data must be Page 0/ Application 2.

Key Management Window



Iris Data Encryption Method

Select the encryption mechanism. Choices include: AES, DES, DES3, and no encryption. Once you change the encryption mechanism, a new key must be generated.

Generate New Key

Automatically generates a new key. The key is visible only when you generate a new key. After that a predefined number of "*" displays instead.

Load Key from File

Allows you to load a key from a file. A stored key is downloaded to Iris Access hardware using IrisICUAdmin.exe utility available on the Supplemental Materials disc. This utility loads the key from the file and then communicates it to the Iris Access hardware.

If you receive a "Failed to load key from file" error, then you selected a file that contains a key type that is different from the specified data encryption method. When this occurs, the key will not be loaded.

Store Key to File

Stores the key in an encrypted file. New files should have the ".dat" extension.

OK

Accepts the encryption method and key changes, and closes the Key Management window.

Cancel

Cancels the encryption method and key changes, and closes the Key Management window.

Add an IrisAccess (iCLASS) Smart Card Format

IMPORTANT: IrisAccess (iCLASS) applications require a Wiegand format where the total number of bits on a card does not exceed 255. Currently, this limitation is superseded by HID Access Control (iCLASS) and IrisAccess (iCLASS) Wiegand record limitations, which is 143. Furthermore, the length of a custom Wiegand format must equal the total Wiegand bits configured on the Identification Control Unit (ICU).

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select a “Iris Access (iCLASS)” from the drop-down.
7. Verify the iris data encryption method is correct. If not, refer to Modify the Encryption Method or Key on page 282.
8. Click [OK].

Modify the Encryption Method or Key

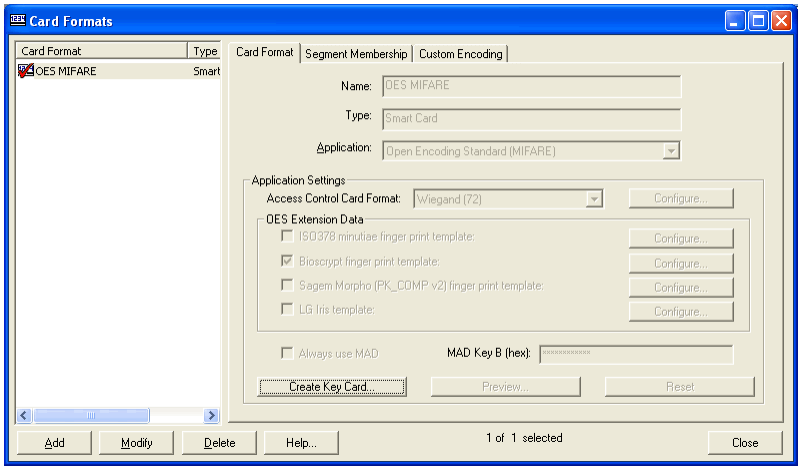
Note: A new key must be generated every time you change the encryption method.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Select the **Iris Access (iCLASS)** card format.
3. Click [Modify].
4. In the Application Settings section, click [Change]. The Key Management window opens.
5. Select the new encryption method from the drop-down.
6. Click either [Generate New Key] or [Load Key from File].
   - If you selected [Generate New Key], a new key is automatically generated. If you want to store the key in an encrypted file, click [Store Key to File], enter the file name and click [Save].
   - If you selected [Load Key from File], navigate to the appropriate file and click [Open].
7. Click [OK] to close the Key Management window.
8. Click [OK] to apply the changes to the IrisAccess card format.

Open Encoding Standard (MIFARE) Card Format Form

The purpose of the Open Encoding Standard (MIFARE) format is to provide cross-vendor badge compatibility of secure MIFARE badge. This means you can choose from different bioscrypt templates to use when creating the card. You can also create a key card which you can use to change the key of an Open Encoding Standard (MIFARE) reader.

This view displays when “Open Encoding Standard (MIFARE)” is selected from the **Application** drop-down.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. Click the corresponding **Configure** button to configure it’s Key A and Key B hex fields and Start sector. Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

ISO378 minutiae finger print template

Select this if you are using the ISO378 minutiae finger print template. Click the corresponding **Configure** button to configure it’s Key A and Key B hex fields and Start sector.

Bioscrypt finger print template

Select this if you are using the Bioscrypt finger print template. Click the corresponding **Configure** button to configure it’s Key A and Key B hex fields and Start sector.

Sagem Morpho (PK_COMP v2) finger print template

Select this if you are using the Sagem Morpho (PK_COMP v2) finger print template. Click the corresponding **Configure** button to configure it’s Key A and Key B hex fields and Start sector.

IrisAccess template

Select this if you are using the IrisAccess template. Click the corresponding **Configure** button to configure it’s Key A and Key B hex fields and Start sector.

Always use MAD

If you select to always use MAD then sector zero stores the application ID that tells the reader what sector to read. When you enable MAD, a new entry is made into the card, if MAD exists on the card. If MAD does not exist, MAD will be created and a new entry made into the card.

MAD Key B (hex)

A covert key for authentication to write to the MIFARE application directory (if MAD is enabled). MAD key B is a 32 character hex value. *Hex values* contain numbers 0-9 and/or letters A-F. By default, this key is set to a secret key.

If MAD already exists on the card then the current MAD key B should be entered. If the user is not an owner of MAD then the user must find out what the current key is before MAD can be written. Once MAD is created, MAD key B will be used if other applications are programmed on to the card. MAD key B should only be released to people who will write other applications.

Create Key Card

Click to open the Encoder Listing window. Select the MIFARE encoder that you are using from the drop-down box and click OK to create a configuration card.

Preview

Click to preview the card layout.

Reset

Click to clear your OES Extension Data selections.

Add an Open Encoding Standard (MIFARE) Smart Card Format

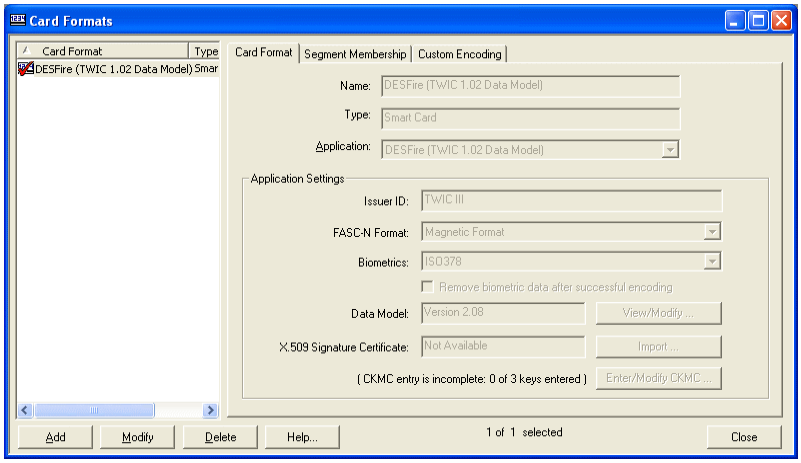
1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.
3. In the listing window, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select “Open Encoding Standard (MIFARE)” from the drop-down.
7. Set the application settings by choosing the access control card format and configuring it.
8. In the OES Extension Data section of the window, select the biometric templates you wish to use and configure them.
9. Optionally, you can choose the MAD settings that are appropriate to what you are doing.
10. Click [OK].

Create an Open Encoding Standard Key Card

1. Click [Create Key Card]. The Encoder Listing window opens.
2. On the Encoder Listing window select the encoder you are using from the **Select encoder** drop-down box.
3. Click [OK].

DESFire (TWIC 1.02 Data Model) Card Format Form

This view displays when “DESFire (TWIC 1.02 Data Model)” is selected from the **Application** drop-down.



Issuer ID

For the TWIC card format you do not need an Issue ID. This is reserved for future use.

FASC-N Format

A customized magnetic card format. A Federal Agency Smart Credential Number (FASC-N) magnetic card format must be created before you configure a government smart card format. All magnetic card formats configured in the system are available from the drop-down.

Biometrics

Choose which biometric you wish to encode onto the card. Your choices include “ISO378 Fingerprint” and “Iris.” You can also choose to encode both by choosing “ISO378 Fingerprint + Iris” from the drop-down box.

Remove biometric data after successful encoding

Select this to remove the biometric information from the system after it’s encoding onto the card.

Data Model

The model that the TWIC card format is encoding. This is as yet not modifiable as only one model is supported.

X.509 Signature Certificate

The signature certificate that is used for particular data models. As only one data model is supported and that does not have an available signature certificate this form element is not used.

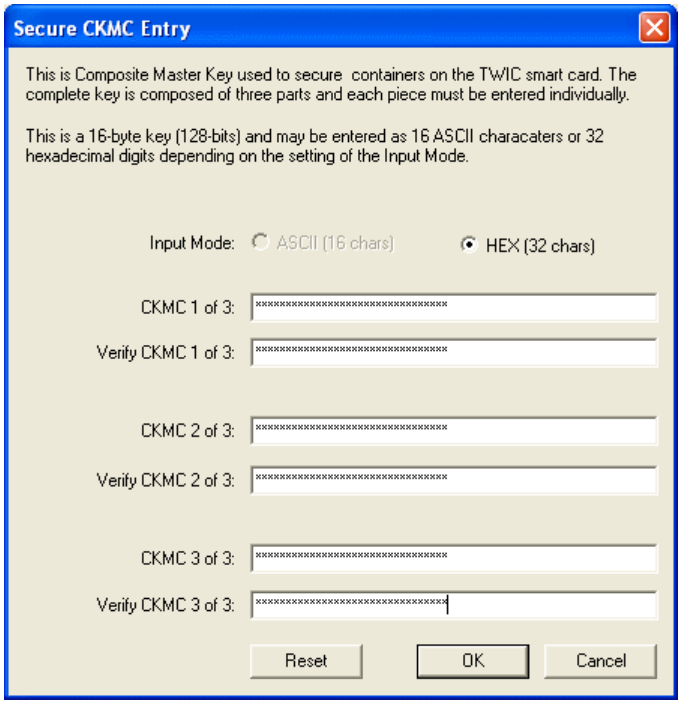
Enter/Modify CKMC

Opens the Secure CKMC Entry window where you can choose to enter the three part composite master key. The text next to this button will change to tell you the CKMC entry is complete once the passwords are entered. This key must match the key set up on the reader.

Add a DESFire (TWIC 1.02 Data Model) Smart Card Format

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens. Select “Smart Card” and click [OK].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. On the Segment Membership tab,. select the segment that this card format will be assigned to.

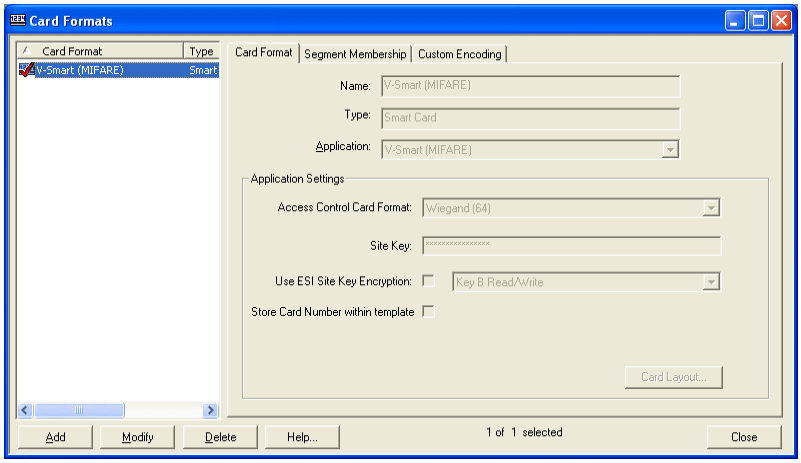
4. In the **Name** field, enter a unique, descriptive name for this format.
5. Select “DESFire (TWIC 1.02 Data Model)” from the **Application** drop-down.
6. In the **FASC-N Format** drop-down box choose “Magnetic Format.”
7. In the **Biometrics** drop-down box choose the biometrics you would like encoded.
8. If you wish, **Check the Remove biometric data after successful encoding** checkbox.
9. Click [Enter/Modify CKMC]. The Secure CKMC Entry window opens.



10. Enter and verify the three key parts.
11. Click [OK]. The Secure CKMC Entry window closes.
12. Click [OK].

V-Smart (MIFARE) Card Format Form

This view displays when “V-Smart (MIFARE)” is selected from the **Application** drop-down.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

Site Key

A key used for authentication. The site key protects bioscrypt data on both types of V-Smart (iCLASS) and V-Smart (MIFARE) card format forms, and can be 16 characters (letters/numbers) or less. The site key must be preprogramed on the reader.

If the card has not been used before, then it is in transport configuration. This means that the card is protected by default keys. Entering the site key overwrites those keys and secures the application. If the card has been written to previously, then the site key must be the key that was used to secure the sectors configured for use with this application. If no site key specified, a blank key will be used.

Site Key Mode

Determines which key becomes the site key, in applications that support both key A and B. If the card is in transport configuration, any key mode can be used. If the card has been previously secured with key A or B, that mode must be selected. Choices include:

- **Hashed (Key B Read/Write)** - applies to V-Smart encoders.
- **Unhashed (Key A Read/Write)** - applies to either GemEasyLink680S or V-Smart encoders. Select this option if you want to read/write to key A.
- **Unhashed (Key B Read/Write)** - applies to either GemEasyLink680S or V-Smart encoders. Select this option if you want to read/write to key B.

This field is configured for V-Smart (MIFARE) card formats only.

Use ESI Site Key Encryption

This check box only applies if you use a V-Smart Bioscrypt encoder. If this box is checked, “Key B Read/Write” is automatically selected in the **Site Key** field and the field is grayed out. Also, during encoding, Key B will be hashed according to the bioscrypt algorithm for hashing keys.

Store Card Number within template

Check this box to encode the badge ID into the Bioscrypt template. If you select this check box, and the **Access Control Card Format** allocates more than 32 bits for the ID number, a prompt will be displayed next to the check box to inform you this format requires the use of the Extended

ID feature which is not currently supported. In this case, do not store the card number within the template.

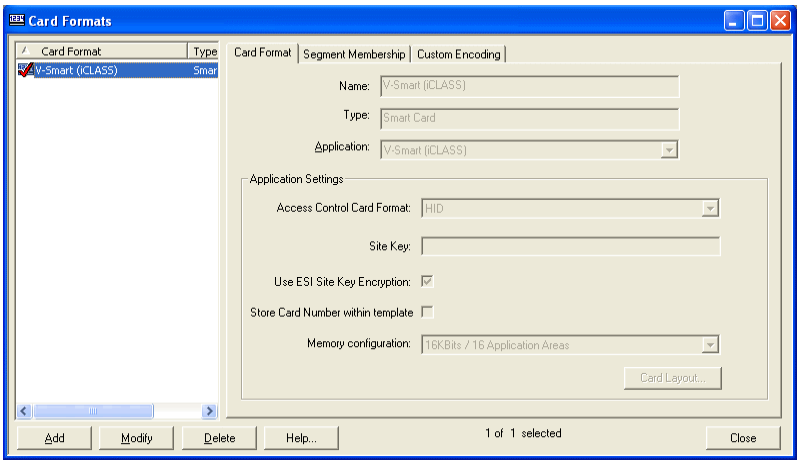
Card Layout

Displays the dialog for both types of V-Smart (iCLASS) and V-Smart (MIFARE) card format forms.

Contact Lenel Technical Support before modifying the default card layout. Changes to the card layout should only be performed by advanced users.

V-Smart (iCLASS) Card Format Form

This view displays when “V-Smart (iCLASS)” is selected.



Access Control Card Format

Lists Wiegand card formats previously configured in the system. The card format selected will be written to the card during encoding. Wiegand card formats with **Special** configured for HID Corporate 1000 cannot be referenced by this smart card format.

Site Key

A key used for authentication. The site key protects bioscrypt data on both types of V-Smart (iCLASS) and V-Smart (MIFARE) card format forms, and can be 16 characters (letters/numbers) or less. The site key must be preprogramed on the reader.

If the card has not been used before, then it is in transport configuration. This means that the card is protected by default keys. Entering the site key overwrites those keys and secures the application. If the card has been written to previously, then the site key must be the key that was used to secure the sectors configured for use with this application. If no site key specified, a blank key will be used.

Site Key Mode

Determines which key becomes the site key, in applications that support both key A and B. If the card is in transport configuration, any key mode can be used. If the card has been previously secured with key A or B, that mode must be selected. Choices include:

- **Hashed (Key B Read/Write)** - applies to V-Smart encoders.
- **Unhashed (Key A Read/Write)** - applies to either GemEasyLink680S or V-Smart encoders. Select this option if you want to read/write to key A.

- **Unhashed (Key B Read/Write)** - applies to either GemEasyLink680S or V-Smart encoders. Select this option if you want to read/write to key B.

This field is configured for V-Smart (MIFARE) card formats only.

Use ESI Site Key Encryption

This check box only applies if you use a V-Smart Bioscrypt encoder. Select if you are using ESI site key encryption.

Store Card Number within template

Check this box to encode the badge ID into the Bioscrypt template. If you select this check box, and the Access Control Card Format allocates more than 32 bits for the ID number, a prompt will be displayed next to the check box to inform you this format requires the use of the Extended ID feature which is not currently supported. In this case, do not store the card number within the template.

Memory configuration

Only displayed on V-smart (iCLASS) card format. Select a preset memory configuration. Choices include:

- 16kbits/16 Application Areas
- 16kbits/16 Application Areas (Custom Key)
- 16kbits/2 Application Areas
- 16kbits/2 Application Areas (Custom Key)

Card Layout

Displays the dialog for both types of V-Smart (iCLASS) and V-Smart (MIFARE) card format forms.

Contact Lenel Technical Support before modifying the default card layout. Changes to the card layout should only be performed by advanced users.

Application License - Bioscrypt

The Bioscrypt Veri-Series Hardware Support (SWG-1402) license is required to use either the V-Smart (MIFARE) or (iCLASS) application.

Add a Bioscrypt Smart Card Format

Notes: This procedure applies to V-Smart (MIFARE) and V-Smart (iCLASS) applications. Both applications require a Wiegand format where the total number of bits on the card does not exceed 64.

Furthermore, to report duress, V-smart card readers must be configured for this in VeriAdmin (Veri-series devices). For more information, refer to the V-Smart Unit Parameter Settings section in the Hardware Installation Guide.

4G V-smart card readers must be configured for this in SecureAdmin. For more information, refer to Enrollment Configuration for V-Station and V-Flex 4G Readers in the Hardware Installation Guide.

1. Choose ***Card Formats*** from the ***Administration*** menu. The Card Formats folder opens.
2. Click [Add]. The Choose Card Format Type window opens.

3. In the listing window, select “Smart Card” and click [OK].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this card format will be assigned to.
   b. Click [OK].
5. In the **Name** field, enter a unique, descriptive name for this format.
6. Select an application from the drop-down.
7. Select “Wiegand (64)” from the **Access Control Card Format** drop-down.
8. Enter a site key.
9. If you are using a V-Smart Bioscrypt encoder and you want key B hashed according to a bioscrypt algorithm, select the **Use ESI Site Key Encryption** check box.
10. If you selected V-Smart (MIFARE) as the application, verify the site key mode is correct. If not, select the correct mode from the drop-down.

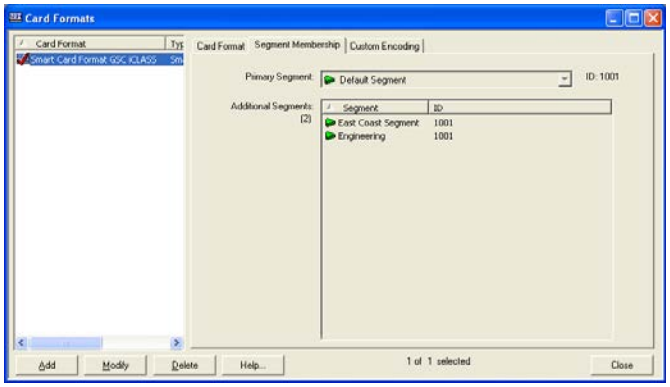
Note: Procedures are not provided for editing the card layout. If you need to do this, contact Lenel technical support.

11. Click [OK].

Segment Membership Form

The Segment Membership form displays if segmentation is enabled on your system.

The fields on the Segment Membership form are disabled when you modify a smart card format that references a Wiegand or magnetic card format. In this case, the smart card format segments are set to the selections of the referenced (Wiegand or magnetic) card format. When a referenced card format’s segments are modified, or when a segment is added to a Wiegand or magnetic card format using the Add Segment Wizard, the segments of any corresponding smart card format is updated.



Primary Segment

The name of the primary segment.

ID

Displays the segment if the segment has an id associated with it. The ID is created automatically when the card format is created. It is the same ID that is displayed in the ID column in the Card Format listing window on the left side of the Card Formats form. This ID needs to be unique to download to access panels.

Different access panels have different maximum allowable card format IDs. Lenel panels support up to eight (ID numbers 1-8) card formats. When card formats are segmented and a format belongs to multiple segments, a unique ID must be obtained for each segment. Depending on which IDs are already in use for each segment, the hardware ID may actually be different for each segment to which the format belongs.

Additional Segments listing window

Displays a listing of additional segments (those other than the primary segment).

Custom Encoding Prerequisites

Several steps must occur in OnGuard to properly encode a magnetic, Wiegand, or smart card. Each step occurs in a different folder in the OnGuard application.

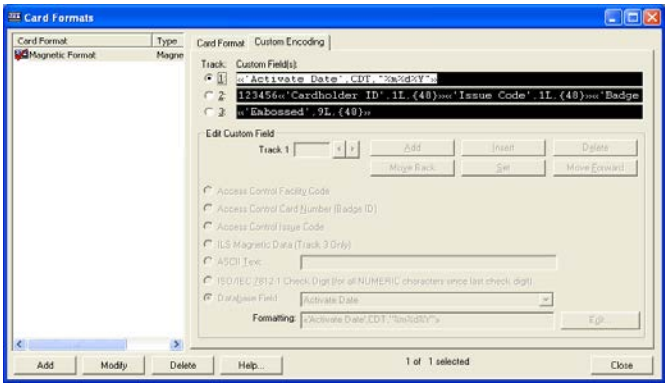
1. In the Workstations folder > Encoding/Scanners form, configure an inline or standalone encoder/scanner.

Note: You do not need to configure USB encoders/scanners (for example, the MIFARE Pegoda contactless smart card reader) in OnGuard applications. Simply install the drivers and attach the hardware to the workstation. This does not apply to the ScanShell 800/1000.

2. In the Card Formats folder, create a card format that will contain data to be encoded on a badge.
3. In the Badge Types folder > Encoding form, assign an encoding format to a badge type. In other words, assign a card format to be encoded on a badge of a specific type.
4. In the Cardholders folder, add a cardholder or visitor record to the database.
5. In Multimedia Capture, capture the cardholder/visitor's photo, signature, and/or biometric data.
6. In the Cardholders folder, encode the badge.

Custom Encoding Form

The Custom Encoding form applies only to magnetic formats. This form is used to modify the information that is encoded on a magnetic card.



Primary Segment

Contains the name of the primary segment.

1

Selecting this button allows you to build a custom expression that will be encoded on track 1.

2

Selecting this button allows you to build a custom expression that will be encoded on track 2.

3

Selecting this button allows you to build a custom expression that will be encoded on track 3.

Track *n*; Field__

Indicates the ordinal number of the currently selected field, and the total number of fields currently in the expression. The format is x/y. For example, "2/3" indicates that the expression contains 3 fields, and that the second of these is the one that's currently highlighted. If there are no fields in the track, this display is not active and the name of the display is Track *n*.

Moves the position of the highlight one field to the left in the expression.

Moves the position of the highlight one field to the right in the expression.

Add

Adds (appends) the selected field to the end of the expression.

Insert

Inserts the specified field to the immediate left of the currently highlighted field in the expression.

Delete

Deletes the selected field from the expression.

Move Back

Moves the currently selected field one position to the left in the expression.

Set

Changes the value of the currently selected field in the expression to a new value you specify.

Move Forward

Moves the currently selected field one position to the right in the expression.

Access Control Facility Code

Adds the facility code access control field to the expression. The field is added as "[AC Facility Code]", and it can be added to the access control track only.

Access Control Card Number (Badge ID)

Adds the facility code access control field to the expression. The field is added as "[AC Badge ID]", and it can be added to the access control track only.

Access Control Issue Code

Adds the facility code access control field to the expression. The field is added as "[AC Issue Code]", and it can be added to the access control track only.

ILS Magnetic Data (Track 3 Only)

Only available to systems with ILS licenses. Only used with track 3, this field allows you to encode ILS lock data on a magnetic card. If you are adding ILS magnetic card data to track 3 by modifying an existing card format and you want to preserve the information encoded on track 1 and track 2 you must first modify the card format and delete any custom field information from track 1 and track 2 and then set the **Total Characters on Track 2** field and all of the **Access Control Fields on Track 2** fields on the Card Format tab to "0". For more information, refer to Configure ILS Custom Encoding on page 1487.

ASCII Text

Includes literal characters in the expression. Enter the actual characters into the **text** field located to the right of the **ASCII Text** field.

ISO/IEC 7812-1 Check Digit (for all NUMERIC characters since last check digit)

If this radio button is selected, a check digit will be applied to all numeric characters added to the expression since the last time a check digit was used.

A *check digit* is a number calculated from the digits of a number and appended to it as a form of integrity check.

Database Field

Includes a field (dynamic data) in the expression. Select the actual field from the **field** drop-down. Only fields currently defined in FormsDesigner and the current date/time field are available for selection.

Formatting

Displays a particular database field reference used in a text/barcode object's text property or a magnetic format's custom encoding.

An "F" appears after the field name in a database field reference when this new FormsDesigner formatting option is selected for it, as shown in the following example: «'Cardholder ID',F»

Edit

Opens the Database Field Properties window (Text/numeric) or (Date/time), in which you can specify field format parameters when custom encoding.

Edit a New Database Field

To edit a new **Database Field** being added to a track on the Custom Encoding form:

1. In the **Database Field** drop-down, select a field to add.
2. Click [Edit]. The Database Field Properties window opens.
3. Make the changes you wish to make, and then click [OK].
4. Click [Add] to add the edited custom field to the end of the track, or [Insert] to insert the edited custom field into the track after the currently selected field.

Edit an Existing Custom Field

To edit an existing custom field in a track on the Custom Encoding form:

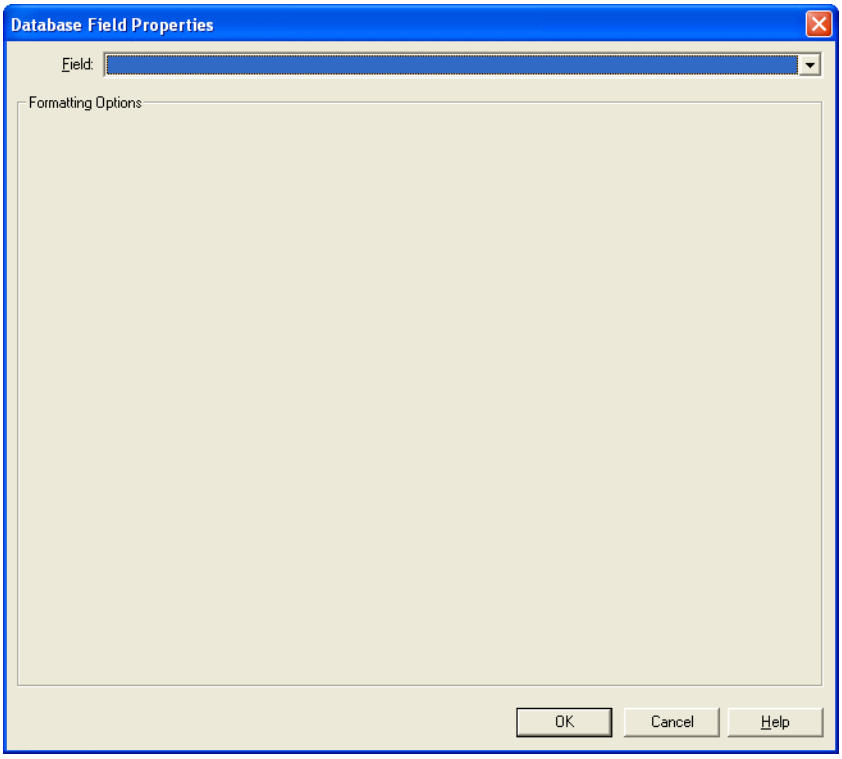
1. Select the **Track** you wish to modify the field(s) for.
2. Use the forward and/or backward arrows to go to the field you wish to modify.
3. Click [Edit]. The Database Field Properties window opens.
4. Make the changes you wish to make, and then click [OK].

5. Click [Set] to modify the selected field.

Database Field Properties Window (Blank)

The Database Field Properties window (Blank) is used to format the fields you inserted into a text object using the Text window or the Text Properties window. The contents of this window changes depending on whether the type of field selected in the **Field** drop-down is blank, text/numeric, or date/time.

The Database Field Properties window (Blank) displays only if the field that was previously specified in the **Database Field** field for the Card Format has been renamed or removed via FormsDesigner since the last time the card format was edited.



Field

Displays a list of the BadgeDesigner database fields that can be linked to the object (including standard BadgeDesigner database fields and user-defined database fields). The contents of the Database Field Properties window changes depending on whether the field selected in this drop-down is blank, text/numeric, or date/time.

OK

Saves the changes you have made and exits the window.

Cancel

Exits the window without saving the changes.

Help

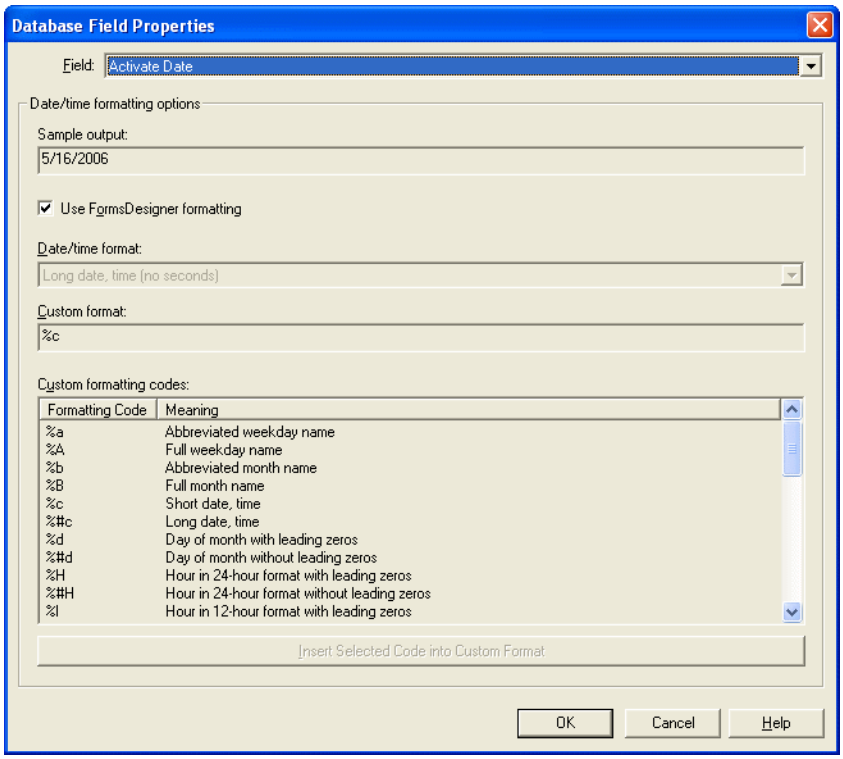
Displays online help for this topic.

Database Field Properties Window (Date/time)

The Database Field Properties window (Date/time) is used to format the date/time database fields you inserted into a text object using the Text window or the Text Properties window. The contents of this window depend on whether the type of value in the **Field** drop-down is blank, text/numeric, or date/time.

Note: In BadgeDesigner, you may select a **Field**; in System Administration and ID CredentialCenter, the **Field** is not available.

The Database Field Properties window (Date/time) displays when a date/time field is specified in the Database Field drop-down on the Custom Encoding tab in the Card Formats folder and then [Edit] is clicked.



Field

Describes the object being modified. The contents of the Database Field Properties window changes depending on whether the field selected in this drop-down is blank, text/numeric, or date/time. In BadgeDesigner, you may select a **Field**; in System Administration and ID CredentialCenter, the **Field** is not available.

Sample output

Displays a sample output of the data. This field is display-only, and is automatically updated as changes are made.

Use FormsDesigner formatting

Check this box to use the field formatting as shown in the Cardholders form. For example, the activate date could appear as “1/1/2001” instead of “Monday, January 01, 2001 12:00 AM.” Newly inserted field references default to having this option checked.

Date/time format

Enabled for selection if the **Use FormsDesigner formatting** check box is deselected. Allows you to choose from a predefined list how the field will be formatted.

Custom format

Enabled for selection if you select “Custom” from the **Date/time format** drop-down. Allows you to design a customized format using the formatting codes.

Custom formatting codes

Enabled for selection if you select “Custom” from the **Date/time format** drop-down. Provides a predefined list of formatting codes you can use to customize the field format.

Insert formatting code

Enabled only when an entry is selected in the **Custom formatting codes** list. Click this button to apply a selected custom formatting code to an output. The **Sample output** field will then be updated with a preview of the output.

OK

Saves the changes you have made and exits the window.

Cancel

Exits the window without saving the changes.

Help

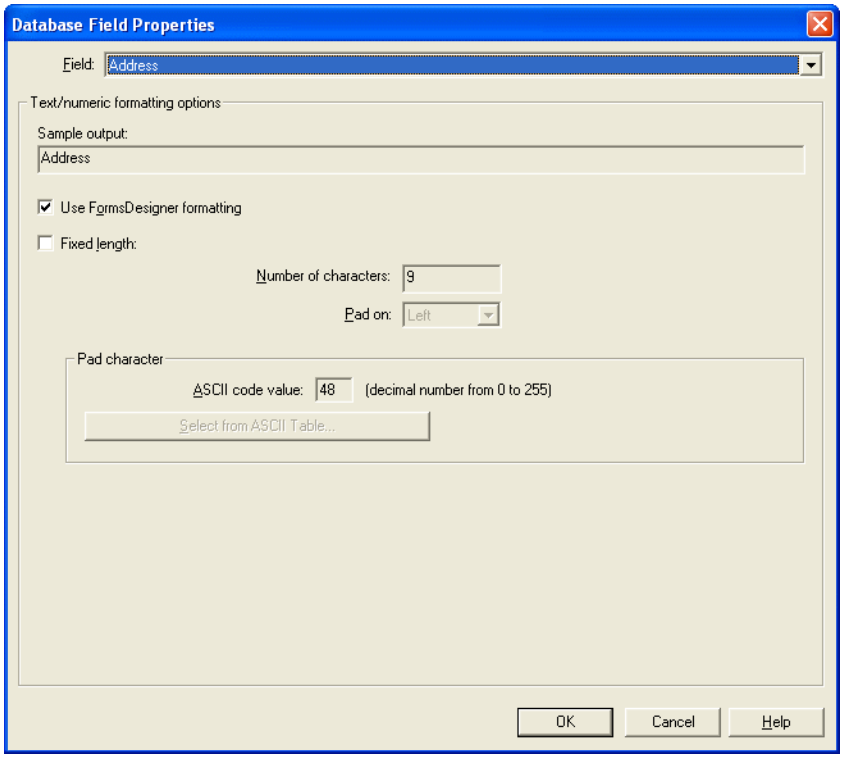
Displays online help for this topic.

Database Field Properties Window (Text/numeric)

The Database Field Properties window (Text/numeric) is used to format the text/numeric database fields you inserted into a text object using the Text window or the Text Properties window. The contents of this window depend on whether the type of value in the **Field** drop-down is blank, text/numeric, or date/time.

Note: In BadgeDesigner, you may select a **Field**; in System Administration and ID CredentialCenter, the **Field** is not available.

The Database Field Properties window (Date/time) displays when a text/numeric field is specified in the **Database Field** drop-down on the Custom Encoding tab in the Card Formats folder and then [Edit] is clicked.



Field

Describes the object being modified. The contents of the Database Field Properties window changes depending on whether the field selected in this drop-down is blank, text/numeric, or date/time.

In BadgeDesigner, you may select a **Field**; in System Administration and ID CredentialCenter, the **Field** is not available.

Sample output

Displays a sample output of the data. This field is display-only, and is automatically updated as changes are made.

Use FormsDesigner formatting

Check this box to use the field formatting as shown on the Cardholder screen. For example, the phone number could appear as “(123) 456-7890” instead of “1234567890.” The field defaults to having this option checked.

Fixed length

Check this box if the field data should contain a specific number of characters/numbers.

Number of characters

Specify the number of characters or numbers in this field.

Pad on

Pads or truncates fields on the left or the right. When the **Fixed length** check box is selected, field data will be truncated on the left/right if the cardholder’s data for that field exceeds the specified number of characters. If the cardholder’s data for that field is less than the specified number of characters the field data will be padded on the left/right.

ASCII code value

Using ASCII Code, choose the pad character. If the data is padded on the left, the pad character(s) will show up before the data. If the data is padded on the right, the pad character(s) will show up after the data.

Select from ASCII Table

Brings up the Select Decimal ASCII Code dialog and allows you to select the pad character from a list.

OK

Saves the changes you have made and exits the window.

Cancel

Exits the window without saving the changes.

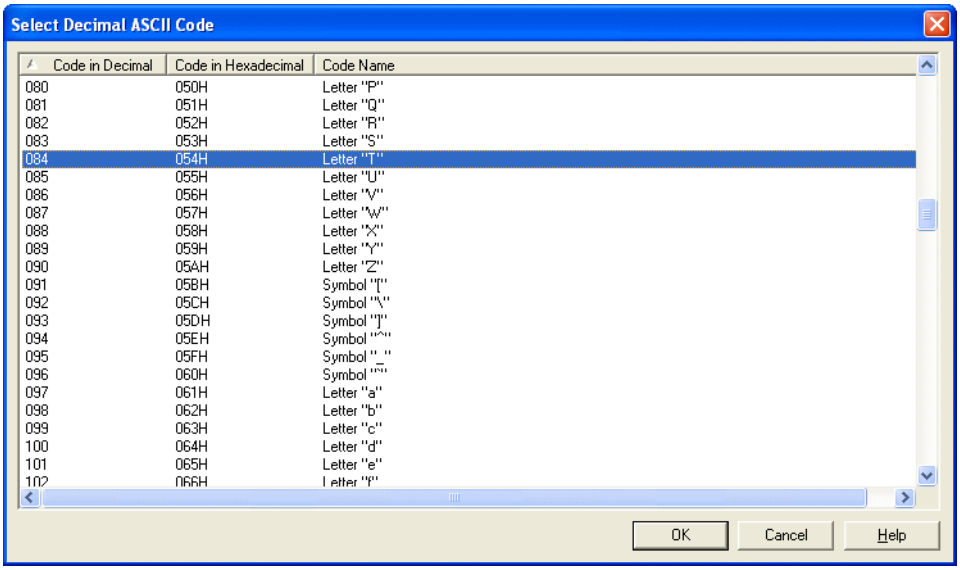
Help

Displays online help for this topic.

Select Decimal ASCII Code Dialog

The Select Decimal ASCII Code dialog lists all ASCII codes in decimal and hexadecimal, as well as the code name for each.

The Select Decimal ASCII Code dialog is by clicking the [Select from ASCII Table] button on the Database Field Properties window (Text/numeric).



Code in Decimal

Lists the code for the decimal (base-ten) representation of the character(s).

Code in Hexadecimal

Lists the code for the hexadecimal (base-sixteen) representation of the character(s).

Code Name
Lists the international standard character name.

OK
Once you have selected an ASCII code, click this button to save the changes and exit from this window.

Cancel
Exits the window without saving the changes.

Help
Displays online help for this topic.

Custom Encoding Procedures

Use the following procedures for this dialog.

Build a Custom Expression: Process Outline

General guidelines for custom encoding are given below. The specific procedure is determined by what you want to encode and where. To help you, a detailed custom encoding example follows this procedure.

1. When adding or modifying a magnetic card format, select the Custom Encoding tab.
2. Choose a track number by selecting the **1**, **2**, or **3** radio button.
3. For each track:
   a. In the Edit Custom Field section, select the appropriate field type radio button.
   b. If necessary provide specific information. For example, if you select the **Database Field** radio button, select the database field from the drop-down and click [Add].
   c. Repeat steps a-b for each custom field you want to add. Refer to Modify a Custom Expression on page 299 for tips on using the Custom Encoding form.
4. Repeat steps 2 and 3 for each track to be encoded.
5. Click [OK].

Modify a Custom Expression

Refer to the following tips when modifying a custom expression:

- If you make a mistake when specifying a field, simply navigate to the field you wish to change, make the change then click [Set] to register the change.
- If you forget to insert a specific field, simply navigate to the left of where you want the field to be placed, select the field, then click [Insert] to insert the missing field.
- If you place a field out of sequence, simply navigate to that field then click [Move Back] or [Move Forward] to reposition the field within the track. (You cannot move a field to another track.)
- The currently selected field appears as black characters against a white background. All other fields in the encoded expression appear as white characters against a black background.
- On the Custom Encoding form, the three access control field radio buttons are always dimmed when a track other than the access control track is selected. Because the access control readers

look for access control fields only on the access control track, these fields can't be encoded on any other tracks.

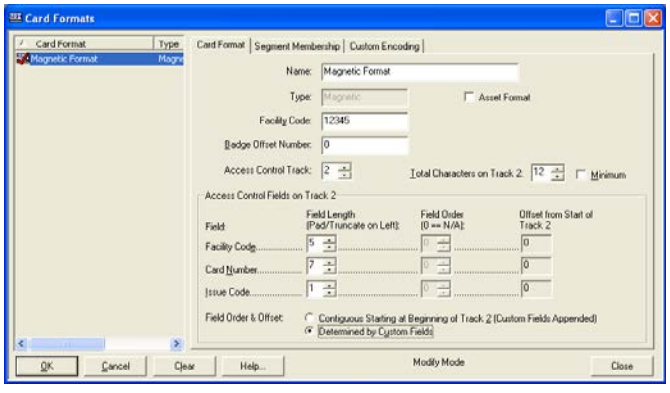
Custom Encoding Example

Lets say you want to encode the following information on magnetic cards:

- Track 1: the cardholder's first, middle, and last names (database fields), each separated by a caret (^)
- Track 2: an ISO 7812-1 standard encoded track containing the following items in the order listed:
  - a 6-digit card issuer number (123456 in our example)
  - the rightmost digit of the cardholder ID (database field)
  - the rightmost digit of the issue code access control field
  - the card number access control field, a 7-digit fixed length number with leading zeros
  - an ISO/IEC 7812-1 check digit for all previous digits on the access control track
- Track 3: the cardholder's embossed value (database field), a 12-digit fixed length number with leading zeros

Note: The access control fields are specified in the custom encoding. The card readers will ignore fields encoded on tracks 1 and 3 and the following custom fields encoded on the access control track: the 6-digit card issuer number, the rightmost digit of cardholder ID and the check digit.

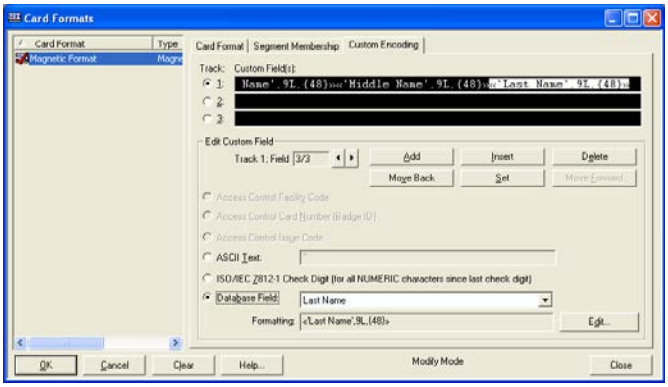
1. Indicate that you want to customize a magnetic format. To do this:
   a. In the Card Format listing window, select the "Magnetic Format" entry that you want to custom encode.
   b. Click [Modify].
2. Select the **Determined by Custom Fields** radio button. This tells the system that the position of the access control track access control fields will be specified on the Custom Encoding form. All fields in the **Field Order (0 == N/A)** and **Offset from Start of the access control track (Characters)** sections are reset to zero since there are no access control fields in the access control track custom encoding yet.
3. In the Field Length (Pad/Truncate on Left) section, set the card number to "7". The issue code should already be set to "1". You should see the following at the end of this step:



4. Select the Custom Encoding tab.
5. Add the cardholder's first name field to track 1. To do this:

a. Select the track **1** radio button.
b. Select the **Database Field** radio button.
c. From the drop-down, select “First Name.”
d. Click [Edit]. The Field Format window opens.
e. Deselect the **Fixed Length** check box.
f. Click [OK].
g. Click [Add]. This inserts an expression for the First Name field into custom field 1.

6. Append a caret (^) field separator character to track 1. To do this:
   a. Click the **ASCII Text** radio button.
   b. In the text field, enter the caret character, ^. (If there is already information in this field, replace it with the caret character by highlighting the information, then enter the caret character in its place.)
   c. Click [Add].
7. Repeat step 5, but instead select the “Middle Name” database field to append the middle name field to track 1.
8. Append a caret field separator character to track 1 by repeating step 6.
9. Repeat step 5, but instead select the “Last Name” database field to append the last name field to track 1. You should see the following at the end of this step:



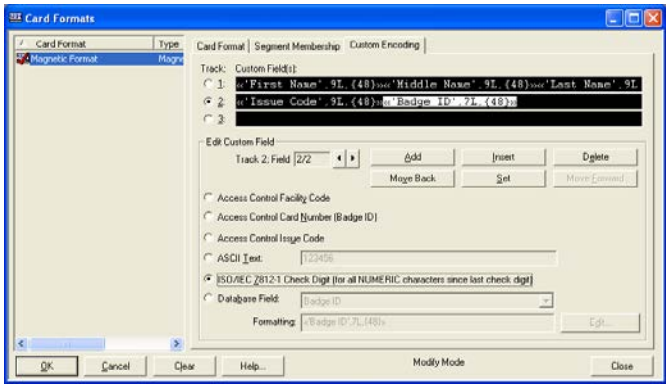
10. Add the card issuer ID “123456” to the access control track. To do this:
    a. Select the track **2** radio button.
    b. Select the **ASCII Text** radio button.
    c. In the text field, enter “123456.”
    d. Click [Add].
11. Append the rightmost digit of the cardholder ID field to the access control track. To do this:
    a. Select the **Database Field** radio button.
    b. From the drop-down, select “Cardholder ID.”
    c. Click [Edit]. The Field Format window opens.
    d. Select the **Fixed Length** check box.
    e. In the **Number of characters** field, enter “1.”
    f. Select “Left” from the **Pad on** drop-down.
    g. Click [OK].

h. Click [Add]. Since you've specified that only 1 character is allowed for this field, and have set the field to pad/truncate on the left, all but the last digit will be truncated. This leaves only the rightmost digit of the cardholder ID field, which is what you wanted to encode here.

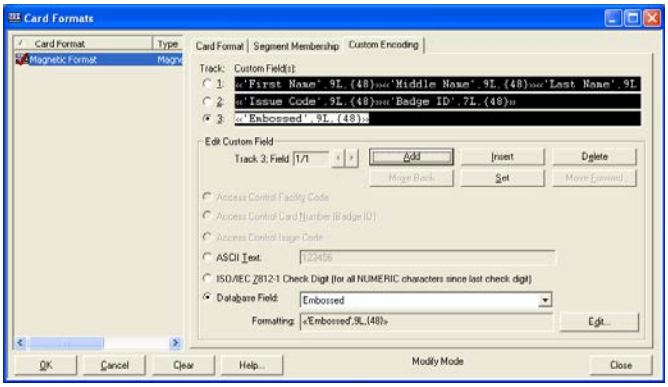
12. Append the issue code access control field to the access control track. To do this:
    a. Select the **Access Control Issue Code** radio button.
    b. Click [Add].

Note: The **Access Control Issue Code** radio button is now dimmed, because you can specify the issue code field for access control only once on the access control track.

13. Append the card number access control field to the access control track. To do this:
    a. Select the **Access Control Card Number (Badge ID)** radio button.
    b. Click [Add].
14. Append an ISO/IEC 7812-1 check digit character to the access control track. To do this:
    a. Select the **ISO/IEC 7812-1 Check Digit (for all NUMERIC characters since last check digit)** radio button.
    b. Click [Add]. You should see the following at the end of this step:



15. Add the embossed field to track 3 as a 12 digit fixed length number with leading zeros. To do this:
    a. Select the track **3** radio button.
    b. Select the **Database Field** radio button.
    c. From the field drop-down, select "Embossed."
    d. Click [Edit]. The Field Format window opens.
    e. Select the **Fixed Length** check box.
    f. In the **Number of characters** field, enter "12."
    g. Select "Left" from the **Pad on** drop-down.
    h. Click [Select]. The Select Control Character window opens.
    i. From the listing window, select "0" (the zero character).
    j. Click [OK].
    k. Click [OK] on the Field Format window.
    l. Click [Add]. You should see the following at the end of this step:



16. Click [OK]. The card format is now configured for the specified custom encoding. However, you must download this card format to the card readers before the application can use it.

Encode the Example Card Format

The application encodes magnetic information on ID cards using the ISO 7811 magnetic encoding standard, described in the following table.

ISO 7811 Track Format Standard

Track	Magnetic Format	Typical Use
1	IATA	financial
2	ABA	security
3	TTS	none

For MAGICARD and NISCA PR5100 printers, the application automatically sets the track 1, 2, and 3 magnetic formats to IATA, ABA, and TTS respectively. The application assumes that these track formats are already configured on other card printers. Most printers have either a Windows driver or a Windows diagnostic program (as does the DataCard (r) printer) that enables you to specify the track formats.

The track's magnetic format dictates the number of bits per character, the bits per inch, the start sentinel character, the set of ASCII characters allowable on the track, and the maximum number of characters per track. The following table provides details.

ISO 7811 Magnetic Track Formats

Property	Magnetic Format		
	IATA	ABA	TTS
Bits/Character	7	5	5
Bits/Inch	210	75	210
Start Sentinel Character (SS)	%	;	;

ISO 7811 Magnetic Track Formats (Continued)

Property	Magnetic Format		
	IATA	ABA	TTS
End Sentinel Character (ES)	?	?	?
Field Separator Character (FS)	^	=	=
ASCII Chars Allowed on Track	SPC ! ‘ # $ % & ‘ ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _	0 1 2 3 4 5 6 7 8 9 : ; < = > ?	0 1 2 3 4 5 6 7 8 9 : ; < = > ?
Max # of Data Chars	76	37	104

The application automatically encodes the start sentinel and end sentinel characters. You must specify the data characters, optional ISO 7812-1 check digit character, and optional ISO 7811 field separator character(s), using the Magnetic Card Format form.

OnGuard supports non-standard track configuration on some printers. For more information please refer to Appendix H: Inline Encoding on page 1443.

Card Format Folder Procedures

Use the following procedures for this folder.

Modify a Card Format

Note: The fields on the Segment Membership form are disabled when you modify a smart card format that references a Wiegand or magnetic card format. In this case, the smart card format segments are set to the selections of the referenced (Wiegand or magnetic) card format. When a referenced card format’s segments are modified, or when a segment is added to a Wiegand or magnetic card format using the Add Segment Wizard, the segments of any corresponding smart card format will also be updated.

1. In the listing window, click on the name of the card format that you want to modify.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Card Format

1. In the listing window, click on the name of the card format that you want to delete.

2. Click [Delete].
3. Click [OK]. A confirmation message will be displayed.
4. Click [Yes].

CHAPTER 12

Badge Types Folder

The Badge Types folder contains forms with which you can:

- Define badge types, each consisting of front and back badge layouts, a deactivation date, and an access group
- Identify segments a badge type belongs to
- Assign an encoding format and a badge printer to a badge layout
- Specify required fields for Cardholder records of a given badge type
- Configure ID allocation parameters and badge deactivation status settings for badge types

The folder contains several forms: the Badge Type form, Segment Membership form (if segmentation is enabled on your system), Printing form, Encoding form, Required Fields form, Badge ID Allocation form, Logical Access form, and the Deactivation Settings form. Any form is editable when the folder is in add or modify mode.

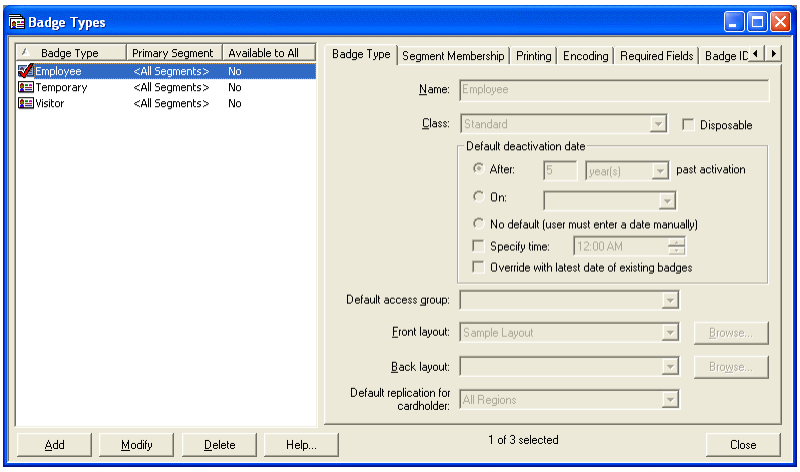
This folder is displayed by selecting ***Badge Types*** from the ***Administration*** menu, or by selecting the Badge Types toolbar button.

Toolbar Shortcut

Note: For segmentation users, badges can be segmented via the Badge Types folder. When badges are segmented via Badge Types folder, they can belong to <All Segments>, one segment or many segments. They can also be assigned to Segment Groups. When badge types are segmented, cardholders' badges are in effect segmented as well, by virtue of their badge type.

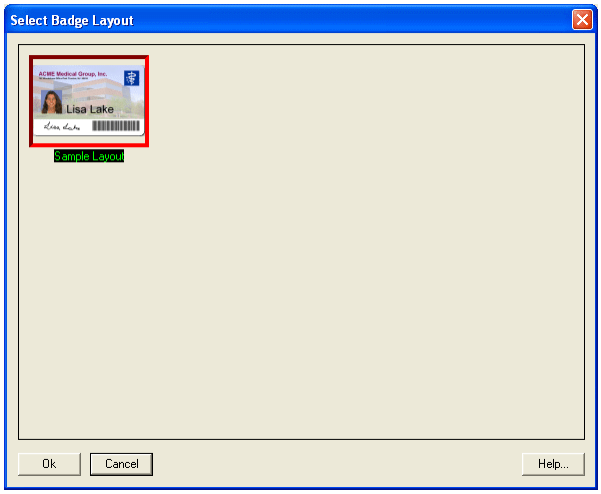
Badge Type Form

The Badge Types form is used to define badge types, each consisting of front and back badge layouts, and a badge deactivation date. If your installation includes the System Administration application, the Badge Type form also includes a default access level group.



Select Badge Layout Window

This window is displayed by clicking the [Browse] button on the Badge Type form.



Badge Type listing window

Lists the names of all currently defined badge types.

Name

Enter a unique, descriptive name for the badge type. When you add a Badge record in the Cardholders folder, you select a badge type by the name defined here.

Class

Indicates the class of the badge. Choices include:

- **Standard** - A standard badge, typically permanently assigned to cardholders.
- **Visitor** - A badge used for visitors. A badge must have this class to be assigned to a visitor.
- **Temporary** - A badge used for temporary assignment to cardholders.

A badge must have a badge type with a class of Visitor or Temporary in order to be automatically moved from one person to another. In previous releases, you could move a badge of any type to another person, since there was no concept of badge class. If you have upgraded from a previous

release, you may want to examine your current badge types and decide which should be changed to a Visitor or Temporary class.

Special Purpose - An ILS badge that serves a special function such as blocking or unlocking a door in an emergency. Special purpose cards are not added to the active badge count of the cardholder For more information, refer to ILS Special Purpose Cards on page 1511. This option is only available with an ILS license.

Disposable

Enabled (allowing selection) only when Visitor is selected in the **Class** field.

- If checked, the visitor's badge will be a disposable badge. When checked, the **Default Access Group** field will become grayed out.
- If not checked, the visitor's badge will not be a disposable badge. A **Default Access Group** field can be selected.
- If a badge type has its Class set to a Visitor, it can be marked as disposable. A disposable badge can be printed but cannot have access levels assigned to it. A disposable badge will not use up a badge ID from the pool of possible IDs for non-disposable badges.
- The Visitor Management application will only allow you to assign badges with a badge type in the Visitor class. Furthermore, it can only print badges with a Disposable badge type attribute.

Default deactivation date

Includes the **After x days/months/years past activation**, **On Specific Date**, **No default (user must enter a date manually)**, and **Override with latest date of existing badges** fields. **Default Badge Deactivation Date** sets the date, with respect to the activation date, on which badges having this Badge Type will expire. When you add a Badge record and select a Badge Type, the Deactivate field will display the date determined by this field. However, you can change the deactivation date for individual badge records.

After x days/months/years past activation

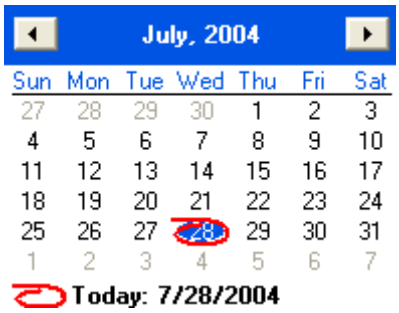
Choose this to specify a Default Badge Deactivation Date that is some number of days/months/years after the activation date (indicate the quantity in the quantity box).

On

Select this radio button if you want to enter a specific date for the default badge deactivation date. The date is selected from the drop-down calendar. If you also want to specify a specific time for default badge deactivation, refer to Specify time on page 310.

Date box

Select a date from the drop-down calendar to be associated with the **On** radio button.



To select a month, click on the and navigation buttons. You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.

Navigate to a year by clicking on the displayed year to access the year spin buttons .

Once you have selected a month and a year, click on the day that you wish the selected badge to deactivate on.

Note: If you select the **On** radio button and "2/5/98" is displayed in the date box, the default badge deactivation date for this badge type will be 2/5/98, regardless of the activation date.

No default (user must enter a date manually)

Select this radio button if you don't want the selected badge to have a default deactivation date. For badge types without default deactivation dates, the user must manually type a date into the **Deactivate** field on the Badge form of the Cardholders folder.

Specify time

Select this check box if you want to specify a specific time for default badge deactivation. When this check box is selected, the **On** radio button cannot be deselected. This field is enabled only when the **Use time** check box is selected on the General Cardholder Options form in the Cardholder Options folder.

Time box

If you selected the **Specify time** check box, enter a time that will be used in conjunction with the selected badge type's default deactivation date.

Override with latest date of existing badges

Select this check box if you want the default deactivation date to default to the latest date of the existing badge.

Default access group

Select a group of access levels to be associated with this badge type. You can change the access levels for an individual cardholder record, using the Access Levels form of the Cardholders folder. The application creates a couple of access levels at installation. Other access levels and access groups are defined in the Access Levels folder of System Administration.

Front layout

Select a badge layout for the front of the card. Badge layouts are defined in the BadgeDesigner application.

Browse

Clicking on this button brings up the Select Badge Layout window, which allows you to select a badge layout for the front from the database.

Back layout

Select a badge layout for the back of the card. Badge layouts are defined in the BadgeDesigner application.

Browse

Clicking on this button brings up the Select Badge Layout window, which allows you to select a badge layout for the back from the database.

Default replication for cardholder

This field only appears on Enterprise systems. Each badge type has a default replication setting. For each cardholder, visitor, and asset record, you can choose if a record is for the Local Region Only or for All Regions. Visitors and assets are not replicated to Regions by default. All records are always replicated to the Master Server.

If adding or modifying a badge on a Master Server, the badge information will go to All Regions. In this case, this field will not be enabled. Settings for this field include:

- Local Region Only - when a badge associated with the selected badge type is added or modified, the information goes to the Master Server only
- All Regions - when a badge associated with the selected badge type is added or modified, the information goes to all regions

Add

Adds a badge type record.

Modify

Changes a badge type record.

Delete

Deletes a badge type record.

Help

Displays online help for this topic.

Close

Closes the Badge Types folder.

Badge Type Form Procedures

Use the following procedures for this form.s

Add a Badge Type

Note: To add a badge type for CMS, refer to Add a Badge Type for CMS on page 1459.

1. In System Administration or ID CredentialCenter, select ***Badge Types*** from the ***Administration*** menu. The Badge Types folder opens.
2. Click the Badge Type tab and click [Add].
3. If segmentation is not enabled on your system, skip this step. If segmentation is enabled, the Segment Membership window opens.
   a. Select the segment that this badge type will be assigned to.
   b. When badge types are segmented, an <All Segments> badge type is considered "administrator only." This means that:
      - Only an <All Segments> user can add, modify, and delete a badge of that type.
      - If cardholders are segmented, only an <All Segments> cardholder can be assigned a badge of that type.
        Select the **Make available to any user and any person (no segment restrictions)** check box if you want to allow the user to lift this restriction on a per badge type basis

so that the <All Segments> badge type is available for assignment by any user to any cardholder (assuming that the user is allowed to update the cardholder record if cardholders are segmented). For more information please refer to Appendix E: Segmentation on page 1411.

Note: This field is enabled only when the selected badge type's primary segment is <All Segments>.

c. Click [OK].

4. Enter a badge type name in the **Name** field.
5. Select a badge class from the **Class** drop-down list. For more information, refer to Badge Type Classes on page 312.
6. Select the **Disposable** check box if you are configuring a visitor badge and do not want to assign access levels.
7. Specify the default deactivation date by completing one of the following:
   - To deactivate a specific amount of time after activation occurs, select the **After** radio button. Select the time period from the drop-down list and enter the amount of time.
   - To deactivate on a specific date and/or time, select the **On** radio button. Choose a date from the drop-down list.
   - To require badge operators to manually enter a deactivation date, choose the **No default (user must enter a date manually)** radio button.
   - To specify a specific time, select the **Specify time** check box and enter the hour and minutes. You may need to first enable the "use time" feature on the General Cardholder Options form. For more information, refer to Chapter 17: Cardholder Options Folder on page 423.
   - To copy the deactivation date of an existing badge, select the **Override with latest date of existing badges** check box.
8. Select a default access group. This field is not available for disposable visitor badge types.
9. Select a front and back layout to be used when printing.
10. Click [OK].

Badge Type Classes

Badge Type Class	Disposable?	Description
Visitor	Disposable	A badge without access levels, assigned to visitors.
	Non-disposable	A badge with access levels, assigned to visitors.
Temporary	Non-disposable	A badge with access levels, used for temporary assignment to employees
Standard	Non-disposable	A badge with access levels, used for permanent assignment to employees.

Modify a Badge Type

1. From the Badge Type listing window, select the badge type entry that you want to change.
2. Click [Modify].
3. Make the changes you want to the fields.

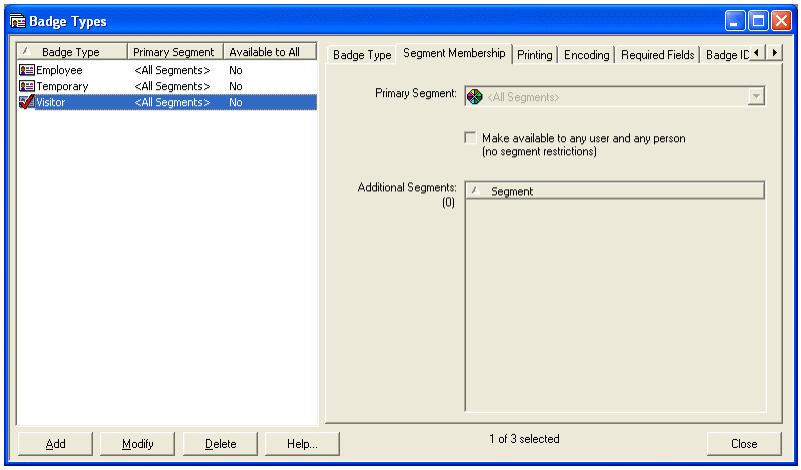
4. Click [OK] to save the changes, or on the [Cancel] to revert to the previously saved values.

Delete a Badge Type

1. From the Badge Type listing window, select the badge type entry that you want to remove.
2. Click [Delete].
3. Click [OK].
4. Click [Yes] to confirm the deletion.

Segment Membership Form

Note: The Segment Membership tab is only displayed if segmentation is enabled on your system.



Primary Segment

Contains the name of the primary segment.

Make available to any user and any person (no segment restrictions)

This field is enabled only when the selected badge type's primary segment is <All Segments>. When badge types are segmented, an <All Segments> badge type is considered "administrator only." This means that:

- Only an <All Segments> user can add, modify, and delete a badge of that type.
- If cardholders are segmented, only an <All Segments> cardholder can be assigned a badge of that type.

Select this check box if you want to allow the user to lift this restriction on a per badge type basis so that the <All Segments> badge type is available for assignment by any user to any cardholder (assuming that the user is allowed to update the cardholder record if cardholders are segmented). For example, in a tenant/landlord scenario, the landlord can create:

- A landlord badge type that is <All Segments> without this check box selected. This badge type could only be assigned to <All Segments> landlord cardholders and modified by landlord users.
- A general visitor badge type that is <All Segments> with this check box selected. Any tenant users could assign this badge type to any cardholder in their segment.

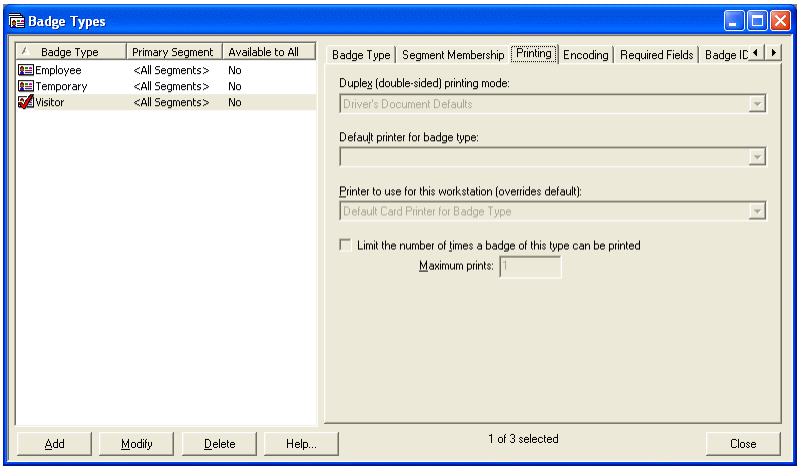
For more information please refer to Appendix E: Segmentation on page 1411.

Additional Segments listing window

Displays a listing of additional segments (those other than the primary segment).

Printing Form

This form is used to assign a badge printer to a badge layout and to limit the number of times a badge type can be printed.



Badge Type listing window

Lists currently defined badge types.

Duplex (double-sided) printing mode

If there is a Back Layout selected for the badge(s), the application allows you to select the orientation (which way the badge is flipped when printed). The options are:

Double-sided Flip Horizontally (Normal): the current card is flipped horizontally before the back layout is printed on its back side. Examples:

- Typical Portrait Horizontal flipping done by card printer drivers:

Front Side: Back Side:

- Typical Portrait Horizontal flipping done by laser printer drivers:

Front Side: Back Side:

- Typical Landscape Horizontal flipping done by card and laser printer drivers:

Front Side: Back Side:

Duplex (double-sided) printing mode (continued)

Double-sided Flip Vertically: the current card is flipped vertically before the back layout is printed on its back side. Examples:

– Portrait Vertical flipping done by card printer drivers: Two single-sided prints or

Front Side: Back Side:

– Landscape Vertical flipping done by card printer drivers: Two single-sided prints or

Front Side: Back Side:

– Typical Portrait Vertical flipping done by laser printer drivers:

Front Side: Back Side:

– Typical Landscape Vertical flipping done by laser printer drivers:

Front Side: Back Side:

Single-sided: the current card is not flipped during printing. If a back layout is selected, the front layout will print on the front of the current card and the back layout will print on the front of the next layout.

Driver's Document Defaults: the duplex mode is set in the printer driver's defaults (set via the Control Panel Printer Applet). Unfortunately horizontal vs. vertical flipping are interpreted differently by different printer drivers. If one type does not work for you, try the other.

Default printer for badge type

Selects the printer that will be used to print cards of the badge type currently selected for all workstations. Options include all printers configured for your computer which are either network printers or local printers which are being shared with the network. Be sure to select a printer that is capable of printing badges.

Printer to use for this workstation (overrides default)

Selects the printer that will be used to print cards from a particular workstation. Options include all local and network printers configured for your computer. This selection overrides all selected "Default Card Printer for Badge Type" if it is different.

Limit the number of times a badge of this type can be printed

Select this check box to limit the number of prints. This feature works in conjunction with the print duplicate badges cardholder badge permission. If a cardholder does not have permission to print duplicate badges the limit on the number of times a badge can be printed does not apply.

Maximum prints

Identifies the maximum number of prints allowed for a badge type. You can enter a value of zero which does not allow anyone to print the badge.

Printing Form Procedures

In OnGuard, badge printers must be assigned to a badge type and/or a workstation. Assigning a printer to a workstation overrides any printer assignment to a badge type.

Modify a Print Setup

1. In System Administration or ID CredentialCenter, select ***Badge Types*** from the ***Administration*** menu. The Badge Types folder opens.
2. Click the Printing tab. Select a badge type and click [Modify].
3. If this badge type has a back layout, select a printing mode from the **Duplex (double-sided) printing mode** drop-down list.
4. Select a default printer for the badge type. Printers must be shared over the network in order to be available from the drop-down list, even if the printer is connected directly to your workstation.
5. Select a printer for the workstation you are currently using.
6. Select the **Limit the number of times a badge of the type can be printed** check box if you want to limit how many times users print a badge type. Enter the maximum number of prints.

Notes:

The number of times a user can print a badge type also depends on their "print duplicate badges" cardholder badge permission setting. For more information, refer to Cardholder Permission Groups Form Procedures on page 366.

If a user attempts to modify the maximum number of prints such that it is lower than the print count of at least one badge of that type then the user will be warned and given the opportunity to cancel the modification.

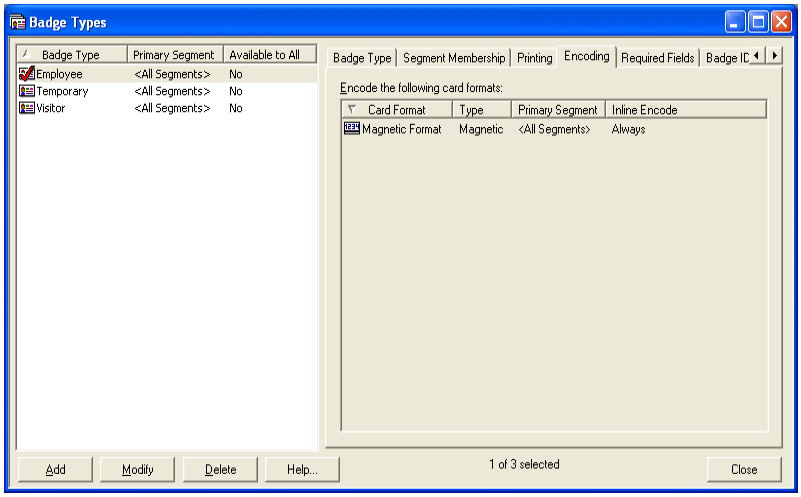
The warning message indicates the number of badges that exceed the attempted new limit and the largest print count for all badges of that type.

7. Click [OK].

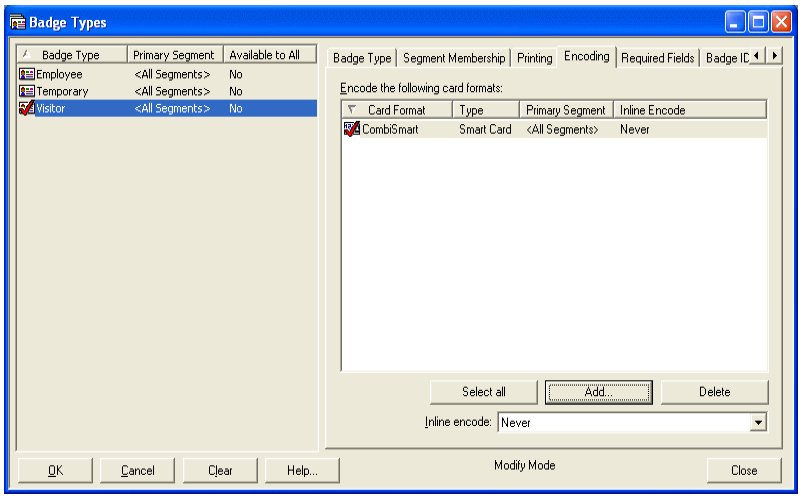
Encoding Form

The Encoding form is used to encode a badge according to the card format that you choose. Different fields display in the Encoding form, depending on the mode you are in (modify mode or view mode).

Encoding Form (View mode)



Encoding Form (Modify mode)



Badge type listing window

Lists currently defined badge types.

Encoding listing window

If you want to encode information on badges of this type, choose a card format from the listing window. Card formats are defined in the Card Formats folder.

Select all

Selects (places a checkmark beside) all the card formats listed in the Encoding listing window

Add

Displays the Add Card Formats dialog where you select the card formats to encode.

Delete

Deletes the selected card format in the Encoding listing window.

Inline encode

Inline encoding is a process of transferring cardholder information to the integrated circuit (IC) or magnetic strip of an ID card during the printing process. Select Always, Never, or If encoder configured from the drop-down list.

Encoding Prerequisites

Several steps must occur in OnGuard to properly encode a magnetic, Wiegand, or smart card. Each step occurs in a different folder in the OnGuard application.

1. In the Workstations folder > Encoding form, configure an inline or standalone encoder/scanner.

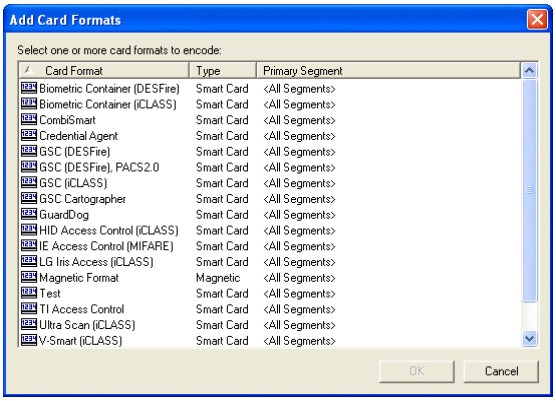
   You do not need to configure USB encoders/scanners (e.g. MIFARE Pegoda contactless smart card reader) in OnGuard applications. Simply install the drivers and attach the hardware to the workstation. This does not apply to the ScanShell 800/1000.
2. In the Card Formats folder, create a card format that will contain data to be encoded on a badge.
3. In the Badge Types folder > Encoding form, assign an encoding format to a badge type. In other words, assign a card format to be encoded on a badge of a specific type.
4. In the Cardholders folder, add a cardholder or visitor record to the database.
5. In Multimedia Capture, capture the cardholder/visitor's photo, signature, and/or biometric data.
6. In the Cardholders folder, encode the badge.

Encoding Form Procedures

Use the following procedures for this form.

Assign an Encoding Format to a Badge Type

1. From the ***Administration*** menu, select ***Badge Types***.
2. Select a badge type and click [Modify].
3. Click the Encoding tab.
4. Click [Add]. The Add Card Formats dialog displays.



5. Select one or more card format(s) and click [OK].

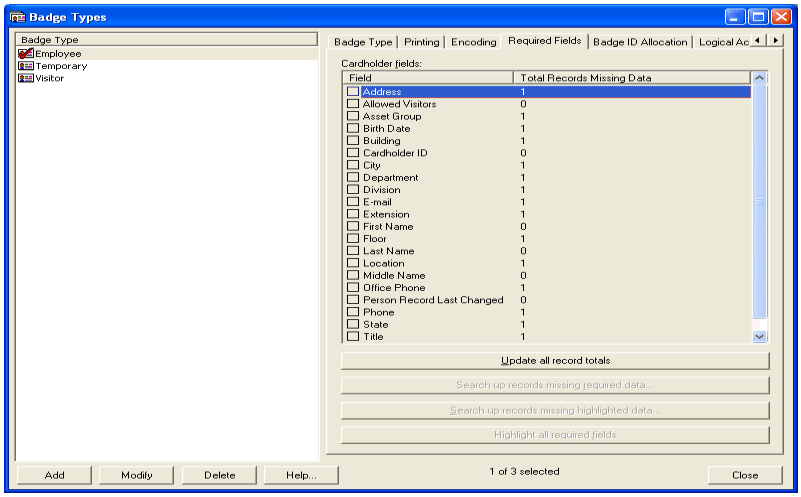
Note: The card formats available for encoding are created in the Card Formats folder. For more information, refer to Card Formats Folder on page 247.

6. Select “Always” from the **Inline encode** drop-down list if you want to transfer cardholder information to the integrated circuit (IC) or magnetic strip of an ID card during the printing process. Otherwise, use the default value, “Never”. A third option, “If encoder configured” can also be used. This will transfer cardholder information if the encoder is configured. This option does not imply that the encoder is actually present and equipped with an encoder that can handle the specific card format.
7. Click [OK].

Required Fields Form

Use this form to specify required fields for cardholder records of a given badge type. Someone adding a cardholder record will be forced to enter data into all of the selected fields before being allowed to assign the selected badge type to the record.

For example, you might require a user to enter a valid **Department** value for a cardholder before allowing the cardholder to be assigned the “Employee” **Badge Type**.



Badge Type listing window

Lists currently defined badge types.

Cardholder fields

Lists all currently defined cardholder record fields. A check box precedes each field name. This field is named **Cardholder Fields** and is populated with cardholder-specific check boxes unless the class of the selected badge type is “Visitor.” In this case, the name of the field changes to **Visitor Fields** and is populated with visitor-specific check boxes.

Update all record totals

Click this button to update the Cardholder fields window. When updated the Cardholder fields window will update to show the total records missing for each data field.

Search up records missing required data

By clicking this button the Cardholders window opens and displays the cardholders who are missing required information.

Search up records missing highlighted data

After highlighting the fields in the Cardholder fields window, click this button to open the Cardholder window and display the cardholders who are missing the highlighted data.

Highlight all required fields

Highlights all the required fields that you've selected. Use in conjunction with the **Search up records missing highlighted data** button.

Required Fields Form Procedures

Use the following procedures for this form.

Specify Required Fields by Badge Type

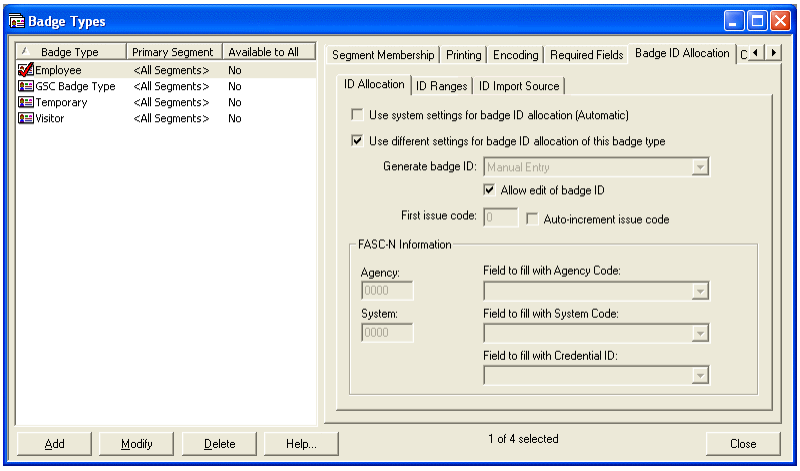
To configure the cardholder and/or visitor fields that will be required when badge operators add a record, complete the following procedure. The fields that will be required depend on the badge type selected during the enrollment process.

1. From the ***Administration*** menu select ***Badge Types***.
2. Select a badge type and click [Modify].
3. Place a checkmark beside any field you want to be required.
4. Click [OK].

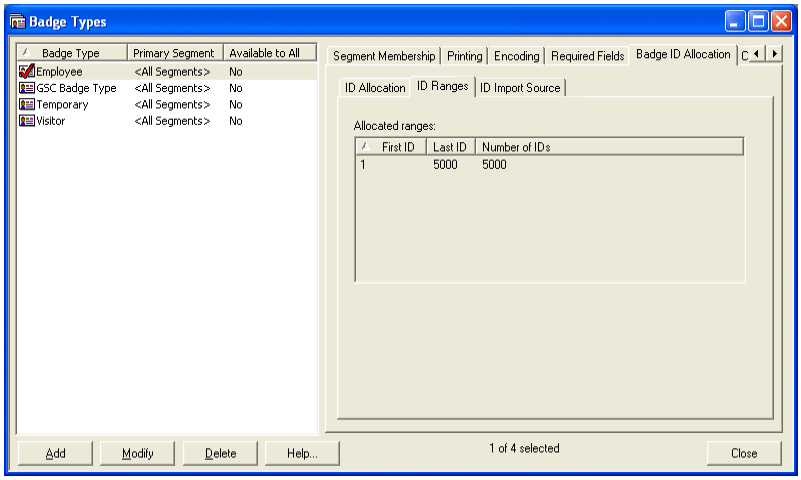
Badge ID Allocation Form

This form is used to configure ID allocation parameters for badge types.

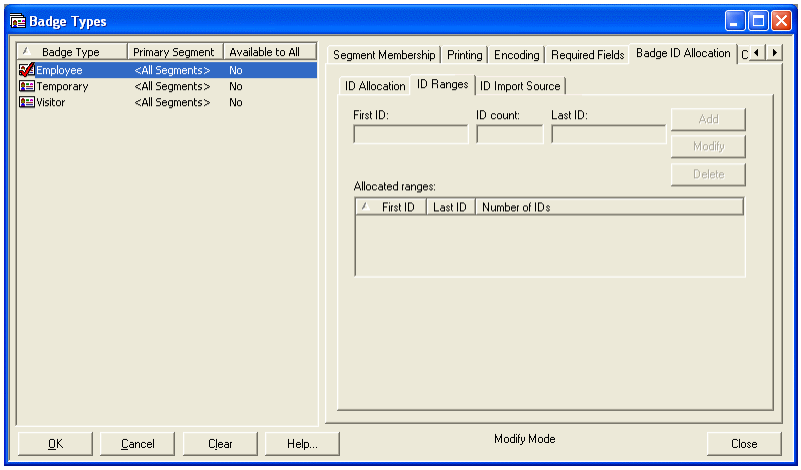
Badge ID Allocation Form - (ID Allocation sub-tab)



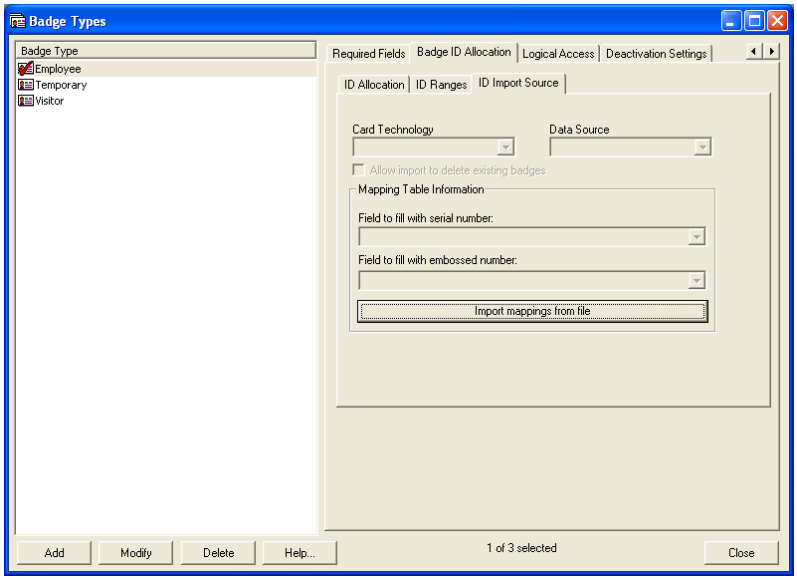
Badge ID Allocation Form - (ID Ranges sub-tab: View Mode)



Badge ID Allocation Form - (ID Ranges sub-tab: Modify Mode)



Badge ID Allocation Form - (ID Import Source sub-tab)



Badge Type listing window

Lists currently defined badge types.

Use system settings for badge ID allocation (Automatic)

When this box is checked, the **Generate badge ID** field, **Allow edit of badge ID** field, **First issue code** field, **Auto-increment issue code** field, and the FASC-N Information section are not enabled. The system settings for badge ID allocation will be used.

Use different settings for badge ID allocation of this badge type

When this box is checked, the **Generate badge ID** field, **Allow edit of badge ID** field, **First issue code** field, and the **Auto-increment issue code** field are enabled.

Generate badge ID

Select the method by which the **Badge ID** field (on the Badge form - modify mode in the Cardholders folder) will be automatically filled in when adding a new badge. Choices include:

- **Automatic** - the badge ID will be assigned by the system. Generally, each new badge ID will be the previous badge ID + 1. This applies even if you are creating a new badge for a cardholder who's already in the database, as would occur if the previous badge were lost or stolen.
- **FASC-N** - Refers to government issued badges. FASC-N is an acronym for Federal Agency Smart Credential Number. Selecting this causes the FASC-N Settings on this form to become enabled for you to use.
- **From 'Cardholder ID'** (or, if you have a custom cardholder layout, the custom field name will be indicated here) - Uses the special cardholder fixed field. (The name of this field may be different if you have a custom cardholder layout designed with FormsDesigner.) Whatever you enter in this field will be used as the badge ID for that particular cardholder. With this setting the badge ID will always be the same for a cardholder - in this case, the issue code is used to distinguish between different badges for the same cardholder.

Note: In order to use this setting the field upon which you are basing the badge ID must be all numeric data.

- **Internal Cardholder ID** - this option is similar to the "From 'Cardholder ID'" option except that this option uses a system-generated number as compared to a manually entered number. Functionally, the badge ID will always be the same for a cardholder. You must use a different issue code to distinguish between different badges for the same cardholder.
- **Import from card** - select this option to enable the **Card Technology** and **Data Source** fields on the ID Import Source tab. Using **Import from card** will import the badge ID from the card. Select the options from the ID Import Source sub-tab to specify how the badge ID will be imported.
- **Manual Entry** - no badge ID will be automatically assigned. A badge ID must be entered by the user who creates the badge record. The badge ID cannot start with a 0 when this option is selected.

Allow edit of badge ID

If selected, a user having the appropriate privileges will be able to modify the badge ID value (on the Badge form via the modify mode in the Cardholders folder). Leave this check box unselected if you want to prevent a user from editing the badge ID.

Note: If badge ID is generated From 'Cardholder ID' or Manual Entry, badge IDs can be edited BEFORE printing. Users with the **Can edit ID/issue/type after printing** permission can also edit badge IDs AFTER printing.

First issue code

If your installation uses issue codes on its badges, zero is used by default as the first issue code when you create a new badge. If your organization wants to use a different number, enter that number in this field.

Auto-increment issue code

You can change this value. However:

- This field is selected by default if you chose “Internal Cardholder ID” in the **Generate badge ID** field.

This field is deselected by default if you chose “Automatic” in the **Generate badge ID** field. This is because each time you create a badge (even if it’s for someone whose badge has been lost), a new badge ID will be assigned automatically. Therefore, it’s considered to be a new card, and the issue code counter starts over again.

Agency

A four digit code identifying the government agency issuing the credential. The agency code is just one part of 31 bits of information that will be encoded on the magnetic stripe of government smart cards. The agency code is also part of what becomes the OnGuard badge ID.

System

A four digit field identifying the system the card is enrolled in. Within an Agency the system must be a unique value. The system is just one part of 31 bits of information that will be encoded on the magnetic stripe of government smart cards. THe system is also part of what becomes the OnGuard badge ID.

Field to fill with Agency Code

Specifies the field in the Cardholders folder > Badge form that will display the Agency Code. You can select from the default OnGuard fields or define a field using FormsDesigner.

Field to fill with System Code

Specifies the field in the Cardholders folder > Badge form that will display the System Code. You can select from the default OnGuard fields or define a field using FormsDesigner.

Field to fill with Credential ID

Specifies the field in the Cardholders folder > Badge form that will display the Credential ID. You can select from the default OnGuard fields or define a field using FormsDesigner.

Allocated ranges listing window

Displays the first and last ID number that will be used, as well as the number of IDs, next ID, and remaining IDs.

First ID (displayed only in modify mode)

Type in the first ID number to be allocated for this badge type. If you enter the first ID and ID count, the last ID will automatically be determined and filled in.

ID count (displayed only in modify mode)

Type in the number of IDs you wish to allocate. If you enter the ID count and first ID, the last ID will automatically be determined and filled in.

Last ID (displayed only in modify mode)

This is the last number that will be allocated as an ID. As long as the **First ID** and **ID count** fields are populated with numeric values, the **Last ID** field will automatically be determined and filled in.

Add (displayed only in modify mode)

This button is enabled only when valid data is entered in the **First ID**, **ID count**, and **Last ID** fields. Its function is to add the range specified in the **First ID**, **ID count**, and **Last ID** fields to the Allocated ranges listing window.

Modify (displayed only in modify mode)

This button is enabled only when an entry is selected in the Allocated ranges listing window. Its function is to modify the range that is selected in the Allocated ranges listing window when a new value is entered in the **First ID**, **ID count**, or **Last ID** fields.

Delete (displayed only in modify mode)

This button is enabled only when an entry is selected in the Allocated ranges listing window. Its function is to delete the range that is selected in the Allocated ranges listing window.

Card Technology

This field is enabled when **Import from card** is selected from the Generate badge ID drop-down box on the ID Allocation sub-tab. Select the card technology that you are using that the badge ID will be imported from.

Data Source

This field is enabled when **Import from card** is selected from the Generate badge ID drop-down box on the ID Allocation sub-tab. Select the data source that the badge ID will be generated from.

- **Card Serial Number** - This option is for importing the badge ID from the serial number of the badge.
- **Mapping Table** - This option allows the badge ID to be imported using the Mapping Table Information. To use this selection, map the serial and embossed numbers to a user-defined field (UDF) on the Cardholders Badge form.

Allow import to delete existing badges

Selecting this check box allows the system to automatically delete badges with the same ID as the newly imported badge, if there were any assigned. If the badges have the same badge ID but different issue codes, they will all still be deleted. This option can only be configured when **Import from card** is selected from the Generate badge ID drop-down on the ID Allocation sub-tab.

Field to fill with serial number

This field is available when **Import from card** is selected from the Generate badge ID drop-down on the ID Allocation sub-tab and when **Mapping Table** is selected for the Data Source. Use this drop-down to select the field to be used for storing serial numbers.

The serial number is obtained from the SERIAL_NUMBER column of the BADGE_ID_IMPORT table. For more information, refer to Import Badge Information for Cards from a Mapping Table on page 327.

A UDF on the Cardholders Badge form should be created for this purpose. The serial number can only be mapped to a text UDF.

Field to fill with embossed number

This field is available when **Import from card** is selected from the Generate badge ID drop-down on the ID Allocation sub-tab and when **Mapping Table** is selected for the Data Source. Use this drop-down to select the field to be used for storing embossed numbers.

The embossed number is obtained from the EXTERNAL_NUMBER column of the BADGE_ID_IMPORT table. For more information, refer to Import Badge Information for Cards from a Mapping Table on page 327.

A UDF on the Cardholders Badge form should be created for this purpose. The embossed number can be mapped to a numeric or text UDF.

Badge ID Allocation Form Procedures

Use the following procedures for this form.

Configure Badge ID Allocation

If you want to configure the ID allocation for a specific badge type, complete the following procedures. If you want to configure the ID allocation for every badge type, refer to the Cardholder Options folder, Badge ID Allocation form.

Note: Changes made to the Badge ID Allocation form in the Badge Types folder override settings on the Badge ID Allocation form in the Cardholder Options folder.

1. Select ***Badge Types*** from the ***Administration*** menu.
2. Select a badge type and click [Modify].
3. Click the Badge ID Allocation tab.
4. Complete one of the following on the ID Allocation sub-tab:
   - Select the **Use system settings for badge ID allocation (Automatic)** check box if you want to use the system settings that are configured in the Cardholder Options folder.
   - Select the **Use different settings for badge ID allocation of this badge type** check box if you want to manually enter configuration settings.
     i. Select the method you will use to generate badge IDs from the **Generate badge ID** drop-down list. For more information, refer to Generate Badge ID Options on page 326.
     ii. Select the **Allow edit of badge ID** checkbox if you want OnGuard users, with the appropriate privileges, to be able to edit badge IDs. If badge ID is generated From 'Cardholder ID' or Manual Entry, badge IDs can be edited BEFORE printing. Users with the **Can edit ID/issue/type after printing** permission can also edit badge IDs AFTER printing.
     iii. Enter the number of the first issue code. Typically this value is zero.
     iv. Select the **Auto-increment issue code** check box if you want the issue code to automatically increment when a new badge is created.
     v. If you selected FASC-N for badge ID generation, enter the four-digit codes identifying the government agency and system issuing the credential. The agency and system codes are encoded on smart cards and become part of the OnGuard badge ID. Select the user-defined fields that will be populated with the agency code, system code and credential ID.
5. On the ID Ranges sub-tab:
   a. Enter the numeric values in the **First ID** and **ID count** fields. The **Last ID** field automatically populates.
   b. Click [Add]. If [Add] is not enabled, you did not enter a valid range.
6. Optionally, on the ID Import Source sub-tab configure the options as you see fit. The options of this tab are enabled when “Import from card” is selected from the **Generate badge ID** drop-down box on the ID Allocation sub-tab.
7. Click [OK].

Generate Badge ID Options

General badge ID	Description
Automatic	Badge IDs are automatically assigned to a cardholder/visitor record. This is the default setting. Each new badge ID is the previous badge ID + 1.
FASC-N	Applies to government issued badges. FASC-N is an acronym for Federal Agency Smart Credential Number.
From "Cardholder ID"	Badge IDs are based on numeric data manually entered in the **Cardholder ID** field in the Cardholders folder. Issue codes differentiate multiple badges for the same cardholder.
Import from card	Badge IDs are created based on information imported from the card. Select the options from the ID Import Source sub-tab to specify how the badge ID will be imported. Selecting this option enables the **Card Technology** and **Data Source** fields on the ID Import Source tab.
Internal Cardholder ID	Badge IDs are based on a system-generated Cardholder ID number. Issue codes differentiate multiple badges for the same cardholder.
Manual	Badge IDs are manually entered by badge operators.

Add a Fixed ID Range

1. Select ***Badge Types*** from the ***Administration*** menu.
2. Click on an entry in the Badge Type listing window to select it.
3. Click the Badge ID Allocation tab.
4. Click [Modify].
5. On the ID Allocation sub-tab:
   a. In the **Generate badge ID** field, select the method you will use to generate badge IDs. The **Generate badge ID** field must be set to "Manual Entry" or "Automatic" to add a fixed ID range.
   b. Depending on your selection, the default settings displayed for the **Allow edit of badge ID** and **Auto-increment issue code** check boxes automatically change. If the check box is enabled, you can change it if you need to.
   c. In the **First issue code** field, enter the number that will be used as the first issue code.
6. On the ID Ranges sub-tab:
   a. Enter numeric values in the **First ID** and **ID count** fields. The **Last ID** field automatically populates.
   b. If you entered a valid range, [Add] will be enabled. Click [Add]. If the fixed ID range does not conflict with a range that already exists, it will be added to the **Allocated ranges** listing window.
7. Click [OK].

Modify a Fixed ID Range

1. Select ***Badge Types*** from the ***Administration*** menu.

2. Click on an entry in the Badge Type listing window to select it.
3. Click the Badge ID Allocation tab.
4. Click [Modify].
5. On the ID Ranges sub-tab:
   a. In the Allocated Ranges listing window, select the fixed ID range to be modified. The values associated with the selected fixed ID range display in the **First ID**, **ID count**, and **Last ID** fields.
   b. Make changes to any of those three fields that you want to change.
   c. Click [Modify].
6. Click [OK].

Delete a Fixed ID Range

1. Select ***Badge Types*** from the ***Administration*** menu.
2. Click on an entry in the Badge Type listing window to select it.
3. Click the Badge ID Allocation tab.
4. Click [Modify].
5. On the ID Ranges sub-tab:
   a. In the Allocated ranges listing window, select the fixed ID range to be deleted.
   b. Click [Delete]. The fixed ID range will be deleted without any confirmation.
6. Click [OK].

Import Badge Information for Cards from a Mapping Table

Before using the Mapping Table as the data source to import the information from a card, the badge information for cards must be imported to the Mapping Table.

1. If desired, use FormsDesigner to create fields for the serial number and embossed number on the Badge form. Create a text field for the serial number. Create a numeric or text field for the embossed number. These fields should have a length sufficient to hold the serial numbers and/or embossed numbers being imported.

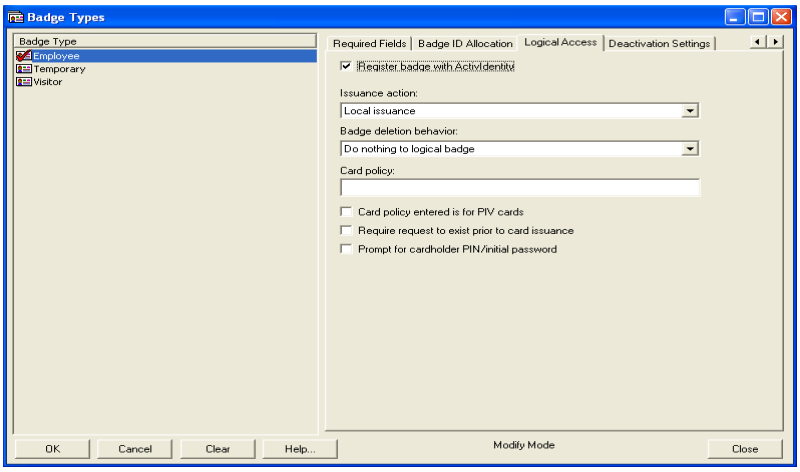
   Note: There is an embossed number field that exists by default. It can be used, provided the length is sufficient. Increase the length of this field, if necessary.

2. In System Administration, configure an iCLASS encoder supporting Badge ID Import. For more information, refer to Configure an Inline or Standalone Encoder/Scanner on page 388.
3. In System Administration > Administration > Badge Types > Badge ID Allocation, select the form's ID Import Source sub-tab, and configure the Data Source on page 324 to use the Mapping Table. If you created the optional fields as described in step 1, then choose the fields created for the serial and embossed numbers.
4. Click [Import mappings from file].
5. Locate and select the file received from HID, and then click [Open] to import the mappings.
6. If the mapping import succeeds, a dialog opens allowing you to inspect and confirm the import.

   If the mappings import fails, you are given the opportunity to verify and update the field names used in the mapping file, and then attempt the import again. The mapping file from HID is human readable, allowing you to verify the field names using a text editor such as Notepad.

Logical Access Form

Use this form to configure the issuance action, badge deletion behavior, and card policy that badge types that will use ActivIdentity CMS.



Register badge with ActivIdentity

This option must be checked to allow issuance and post-issuance (life-cycle management, etc.) operations.

Issuance action

The issuance action defines whether to issue the badge locally or to perform issuance with self-enrollment (i.e., binding; encoding is done by the user with CMS's My Digital ID). Choices include:

- Local issuance - personalizes the smart card (writes data to the card)
- Issuance with self-enrollment (binding) - does not personalize the card (no data is written to the card). Binding only links the card to the user in CMS and allows the user to personalize the card using CMS's My Digital ID.

Note: For CMS version 4.0/4.1: Issuance with self-enrollment (binding) also includes the submission of a badge production request (to define the policy and other information required for self-enrollment).

Badge deletion behavior

Specifies the action that will occur on the logical badge when the physical badge is deleted.

Card policy

Specifies the CMS Policy (configured in CMS) which defines what applications and credentials can be issued to a card by CMS. Be sure to type the policy name correctly; this name is case-sensitive, and must be the same policy name that is configured in CMS.

Card policy entered is for PIV cards

Specifies that the **Card policy** entered is for the issuance of a PIV card. When this option is selected, fingerprint verification is performed immediately after the card is encoded. For more information, refer to Encode/Bind a PIV Card on page 1465 on page 732.

Request request to exist prior to card issuance

Specifies that production requests will be forced prior to card issuance if such requests are submitted by a third party system before OnGuard performs the issuance. If this option is not selected, then OnGuard will submit the production request and immediately execute it.

Notes: For CMS version 4.0/4.1: If this option is not selected, then OnGuard will submit the production request and immediately execute it. However, to ensure compliance with FIPS standards, it is recommended that the production request comes from an authoritative system to the CMS and not from the OnGuard system. **Force request to exist prior to card issuance** should be selected so that the FIPS requirements are met.

For CMS version 3.8: OnGuard always submits the production request. Therefore, **Force request to exist prior to card issuance** should be deselected.

Prompt for cardholder PIN/initial password

Enable to prompt the cardholder to enter their PIN or initial PIN when using their badge.

Logical Access Form Procedures

For instructions on how to configure and use CMS, refer to Appendix I: Integrating ActivIdentity CMS with OnGuard on page 1453.. The following procedure in that section is performed using this form: Add a Badge Type for CMS on page 1459.

Deactivation Settings Form

The deactivation settings are configured system-wide in the Cardholder Options folder, and by badge type in the Badge Types folder. For more information, refer to Cardholder Options Folder on page 423.

First, the deactivation settings for each badge type will be considered. If a badge type has the deactivation setting enabled, the appropriate badges that belong to this badge type meeting the conditions configured will be changed to the new badge status. Then after these steps have been performed, the system setting will be processed.

- All badges that are assigned a badge type with any deactivation settings enabled will be processed first before checking the system setting.
- All badges that are assigned a badge type without any deactivation settings will have the system setting checked when processing badges for deactivation.
- All badges that are assigned a badge type without any deactivation settings, and without the system deactivation setting, will not be included in any of the badge processing.
- When a deactivation setting is chosen for a badge type and the system setting is configured, the badge type setting will be used for any badges belonging to that badge type.

Use or Lose Badge

For use or lose badge, badge deactivation is based on the setting with the lower number of days. Setting either the system setting or badge type setting to zero removes that setting from being processed. For example, if the system setting is zero and the employee badge type setting is 30 days, the use or lose feature will not apply to any badge type except the employee badge type which will

deactivate after 30 days of non use. If the system setting is 30 days and the employee badge type setting is zero, then every badge type will deactivate after 30 days of non use.

- If the number of use or lose days configured for the system setting is less than the number of use or lose days for any badge type setting, the system settings will always override the badge type settings.
- If the number of use or lose days for any badge type is less than or equal to the system setting, the badge type use or lose settings will override the system use or lose settings.

Badge Deactivate Status

The badge deactivate status is based on either the badge type setting or the system badge status setting. If the badge type setting is not set, the system badge status will be used. If neither setting is configured, then the badge status will remain unchanged. The change in badge status occurs between 24 and 48 hours after expiration (accounting for differences in time zones).

If the system setting is configured for new badge status, and the new badge status is configured based on badge type, the setting based on badge type setting will take precedence over the system setting (for that badge type).

Linkage Server

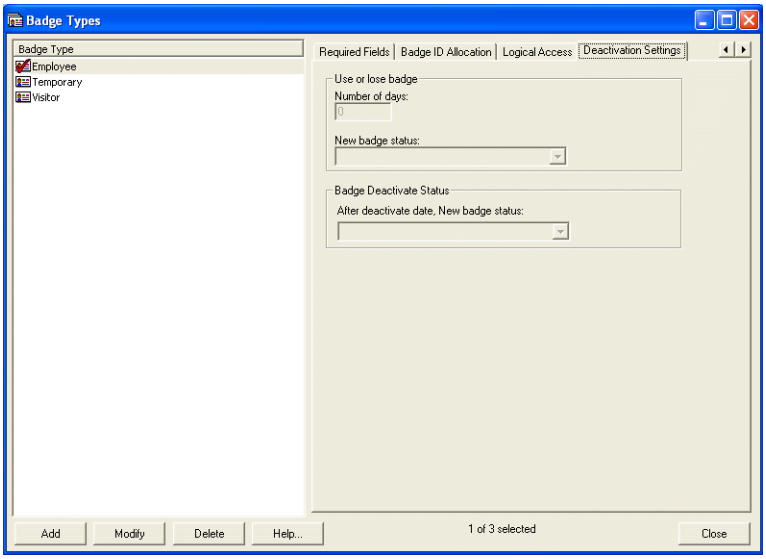
Functionality of deactivation settings requires that the Linkage Server be configured and running.

For Enterprise systems, the Cardholder Options or Badge Type setting will be replicated down to regions. This cannot be modified on the regions.

The actual change in status corresponds to changes to the actual badge and is not replicated, therefore each region must also be running the Linkage Server.

ACS.INI settings are supported. You can configure the Linkage Server host on the General System Options form in the System Options folder. For more information, refer to General System Options Form on page 392. The Linkage Server will run once a day. The following settings can be configured in the ACS.INI file under the `[Service]` section:

Setting	Description
UseOrLoseDebug DeactivateStatusDebug	Used to indicate if a debug file will be created for the use or lose processing or the badge deactivate status processing. It creates a file named UseOrLoseDebug.txt or DeactivateStatusDebug.txt located in the ...\OnGuard\logs directory.
UseOrLoseStartTimeHour DeactivateStatusStartTimeHour	Used to specify the hour (in 24-hour/military time) in which the processing is performed.
UseOrLoseStartTimeMinute DeactivateStatusStartTimeMinute	Used to specify the minute in which the processing is performed.
UserOrLoseDatabaseSleepTime DeactivateStatusSleepTime	Used to specify the database timeout to use for the processing.



Badge Type listing window

Lists currently defined badge types.

Number of days

Enter the number of consecutive days of badge inactivity after which all badges of the selected badge type will be assigned the badge status indicated in the **New badge status** field. A value of zero disables the use or lose badge feature.

New badge status

Enter the badge status that will be assigned to all badges of the selected badge type when the **Number of days** value has been exceeded. Choices in the drop-down list include default badge status values, and any badge status values that were added in the List Builder folder.

After deactivate date, New badge status

Enter the badge status that will be assigned to active badges of the selected badge type when the deactivate date has passed. Choices in the drop-down list include default badge status values except for Active, and any badge status values that were added in the List Builder folder.

Deactivation Settings Form Procedures

Use the following procedures on this form.

Configure Use or Lose Badge Settings

IMPORTANT: Use or Lose Badge functionality relies on Last Location transaction data. If Use or Lose Badge is enabled on an Enterprise system, Last Location information must be exchanged using Replicator at least twice a day. For more information, refer to Replicator Schedule Form in the Replication Administration User Guide.

1. Select ***Badge Types*** from the ***Administration*** menu. The Badge Types folder opens.
2. On the Deactivation Settings tab, select a badge type and click [Modify].

3. In the **Number of days** field, enter the number of consecutive days of badge inactivity after which badges will be deactivated. A value of zero disables the use or lose badge feature, unless the use or lose feature is configured system-wide.
4. In the **New badge status** field, enter the badge status that will be assigned to all badges of the selected badge type when the number of days has been exceeded.

   Choices in the drop-down list include default badge status values (except Active) and any badge status values that were added in the List Builder folder. For more information, refer to Chapter 19: List Builder Folder on page 481.
5. Click [OK].

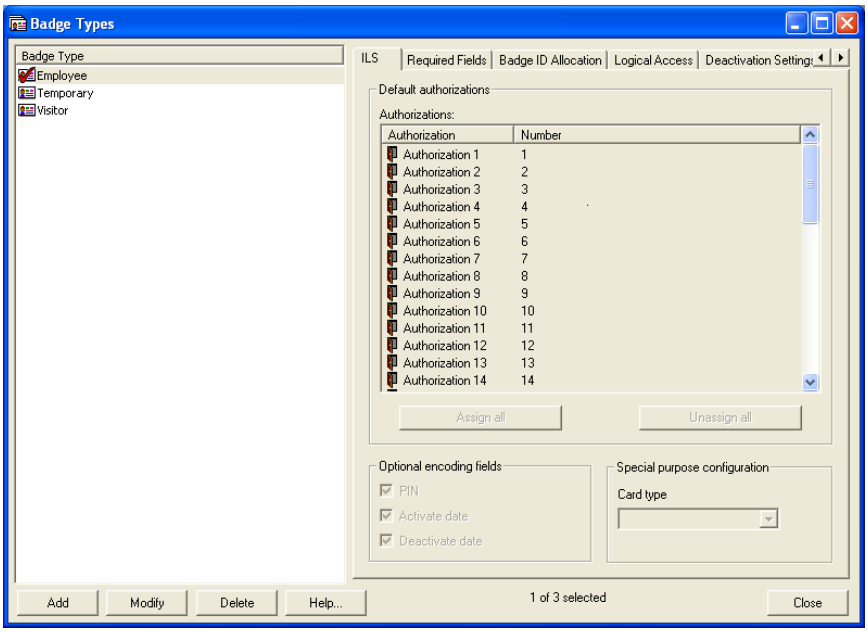
Configure Badge Deactivate Settings

1. Select ***Badge Types*** from the ***Administration*** menu. The Badge Types folder opens.
2. On the Deactivation Settings tab, select a badge type and click [Modify].
3. In the **After deactivate date, New badge status** field, enter the badge status that will be assigned to all badges of the selected badge type when the deactivate date has passed.

   Choices in the drop-down list include default badge status values (except Active) and any badge status values that were added in the List Builder folder. For more information, refer to Chapter 19: List Builder Folder on page 481.
4. Click [OK].

ILS Form

IMPORTANT: To view this form your system must have an ILS license.



Authorizations

List of authorizations that can be selected to be used on the selected badge type. Authorizations are used to limit access to areas without the need to update the locks and allow you to customize accessibility to the locks as needed.

Assign all
Click to select all of the listed authorizations.

Unassign all
Click to deselect all of the listed authorizations.

PIN
Select to encode the badge PIN code onto the badge. ILS locks require a PIN when in one of the following reader modes: Standard, Security, and Security Passage.

Activate date
When selected, the Badge Activate date and time will be encoded in local time. Badge Activate dates and times will not be downloaded to the locks. However, if encoded on the badge the locks will deny access if the time encoded is previous to the current time.

Deactivate date
When selected, the Badge Deactivate date and time will be encoded in local time. Badge Deactivate dates and times will not be downloaded to the locks. However, if encoded on the badge the locks will deny access if the time encoded is previous to the current time.

Card type
When adding a special purpose badge, you will also need to specify the special function configuration for the card. Special functions include the following:

- Blocking
- Emergency Lock
- Emergency Unlock
- Network Join
- Test

For more information, refer to ILS Special Purpose Cards on page 1511.

ILS Form Procedures

To read how to configure an ILS locking system, refer to Appendix K: Lenel ILS (Integrated Locking Solutions) on page 1473..

CHAPTER 13

Directories Folder

The Directories folder contains forms with which you can add, modify, and delete directories.

The Directories folder contains the Directories form. On the Directories form, there are three sub-tabs: General, Authentication, and Advanced. (The Advanced sub-tab is only displayed for LDAP or Microsoft Active Directories.)

This folder is displayed by selecting ***Directories*** from the ***Administration*** menu.

A directory is a database of network resources, such as printers, software applications, databases, and users. A directory service includes both the directory and the services that make the information in the directory available. OnGuard supports the following types of directory services: Microsoft Active Directory, Microsoft Windows NT 4 Domain, Windows Local Accounts, and LDAP (Lightweight Directory Access Protocol).

A directory must be configured in the Directories folder before it can be linked to a user in the Users folder. After a user account has been linked to a directory account, that directory account will be available for selection when that user logs into the system. A user account may be configured to use an internal account, a directory account, or both to login.

Directories Form (General Sub-tab)

The options available on this form change depending on the **Type** of directory selected.

Listing window
Lists the name, type, and host/domain of currently defined directories.

Add
Click this button to add a directory.

Modify
Click this button to change a directory.

Delete
Click this button to delete a directory.

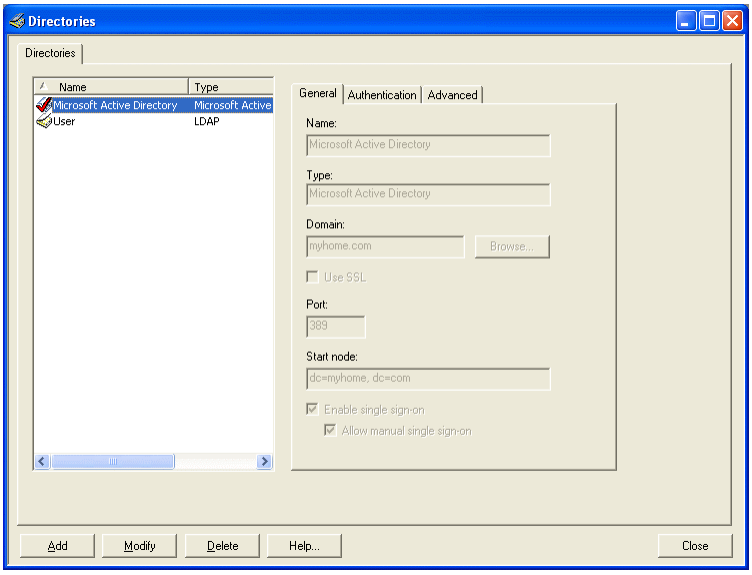
Help

Displays online help for this form.

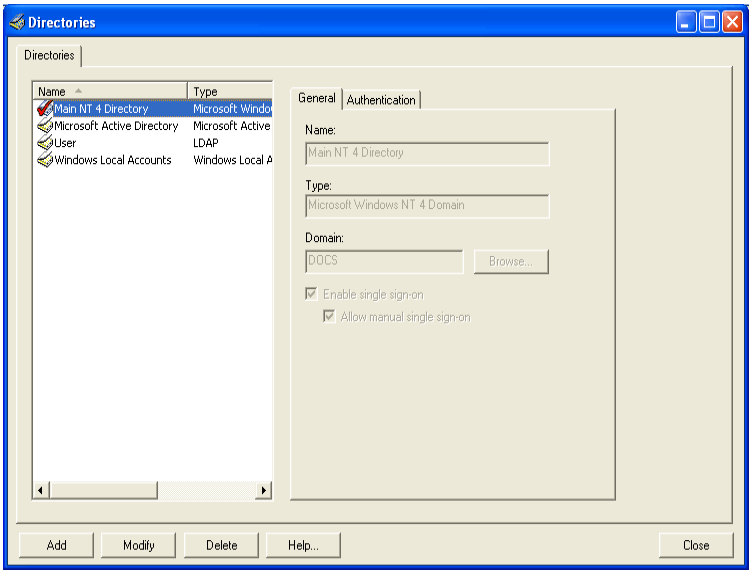
Close

Closes the Directories folder.

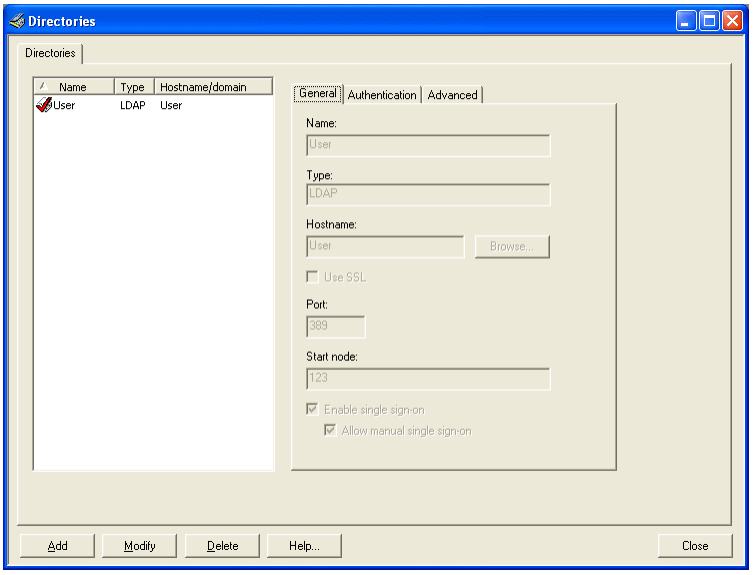
"Microsoft Active Directory" selected as Type



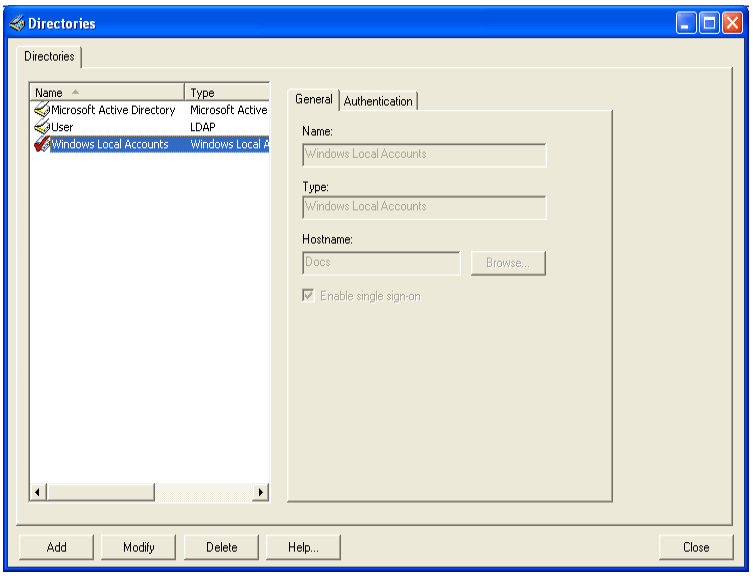
"Microsoft Windows NT 4 Domain" selected as Type



"LDAP" selected as Type



"Windows Local Accounts" selected as Type



Name

Identifies the name of the directory. This is a friendly name assigned to each directory to make it easy to identify. Each name must be unique and can contain no more than 96 characters.

Type

The **Type** is selected in the Add Directory window that is displayed after the [Add] button on the Directories form is clicked. Once selected, the **Type** cannot be modified.

Hostname

Displayed only if the directory **Type** is "LDAP" or "Windows Local Accounts." This is the host name or IP address of the machine running the directory.

Domain

Displayed only if the directory **Type** is “Microsoft Active Directory” or “Microsoft Windows NT 4 Domain.” The **Domain** is the name of the Windows domain, and must be in the following form: tom.windows.accesscontrolsystem.com

Browse

Displays a Browse for computer form from which you can click on the name of a workstation to highlight the entry. Click [OK] to then enter the workstation name in the **Host name**, **Hostname** or **Domain** field, depending on the directory type.

Use SSL

Displayed only if the directory type is “LDAP” or “Microsoft Active Directory.” If selected, SSL (Secure Sockets Layer) will be used. If not selected, SSL will not be used.

Port

Displayed only if the directory type is “LDAP” or “Microsoft Active Directory”. This is the port that the directory listens on for connections.

Start node

(Optional.) Displayed only if the directory type is “LDAP” or “Microsoft Active Directory.” The **Start node** is the node to start searching from, and it is automatically configured. The **Start node** must correspond to the **Domain** specified, and must be in the following form: DC=tom, DC=windows, DC=accesscontrolsystem, DC=com.

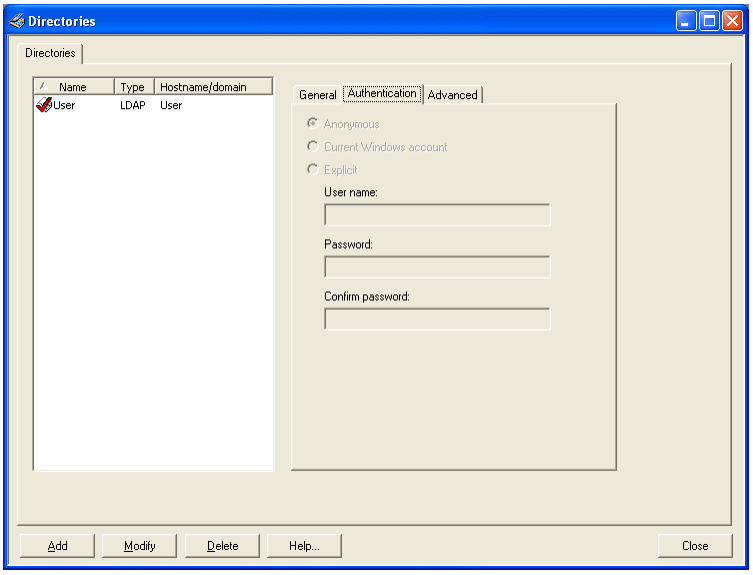
Enable single sign-on

If selected, automatic single sign-on is enabled for the directory.

Allow manual single sign-on

This field is not displayed if the directory **Type** is “Windows Local Accounts.” If selected, manual single sign-on can be used for the directory. For increased security, it is recommended that allow manual single sign-on not be enabled if the directory type is “Microsoft Active Directory” or “Microsoft Windows NT 4 Domain.”

Directories Form (Authentication Sub-tab)



Anonymous

If selected, the user name and password used by OnGuard to connect to the directory will be anonymous.

Current Windows account

If selected, the user name and password used by OnGuard to connect to the directory will be the current Windows account.

Explicit

If selected, specify the **User name**, **Password**, and **Confirm Password** used by OnGuard to connect to the directory.

IMPORTANT: It is recommended that you do not use the explicit user name and password option for authentication to Windows. OnGuard uses reversible encryption (Windows does not), and therefore, Windows passwords should not be stored in the system. If you need to use explicit authentication, you should use an account that only has view permissions to the directory.

User name

(Optional.) The user name to supply the directory service to use for credentials. Must be in the form TOM\tom where TOM is the domain name and tom is the user. It does not need to be an administrative account; it can be a normal network account.

Password

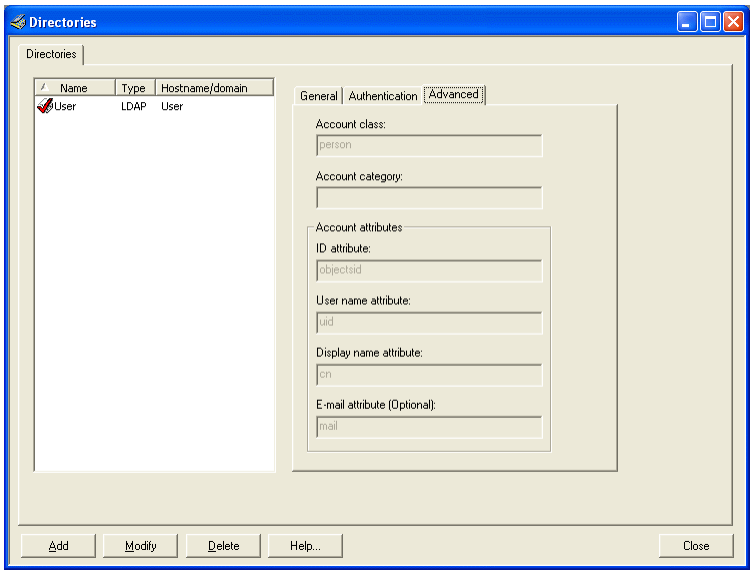
(Optional.) The password to supply to the directory service to use for credentials. Authentication cannot be assigned to a user that does not have a password.

Confirm Password

Enter here exactly the same information that you entered in the **Password** field.

Directories Form (Advanced Sub-tab)

Note: This form is not displayed for directories with the “Microsoft Windows NT 4 Domain” or “Windows Local Accounts” **Type**.



(Displayed only if the directory type is “LDAP” or “Microsoft Active Directory”.)

Account class

The LDAP class that stores account information.

Account category

The account category is used in addition to the account class to improve performance by filtering computers (which are users).

ID attribute

The LDAP attribute of the LDAP Account Class that uniquely identifies an account. This will be used when querying the LDAP directory for the account.

User name attribute

The LDAP attribute of the LDAP Account Class that uniquely identifies an account and is used as a username for the account. This will be used when querying the LDAP directory for the account.

Display name attribute

The LDAP attribute of the LDAP Account Class that is used when displaying the account.

E-mail attribute (Optional)

The E-mail attribute is set to “mail” by default and is available for Microsoft Active Directory and LDAP accounts. Most systems such as Microsoft Exchange Server expose their database objects via directory accounts, but each system may name the e-mail attribute differently. If you add a directory account to the recipient list (on the E-mail form in the Visits folder in OnGuard), that e-mail attribute in the directory is examined, and if it is available, the SMTP address will be returned.

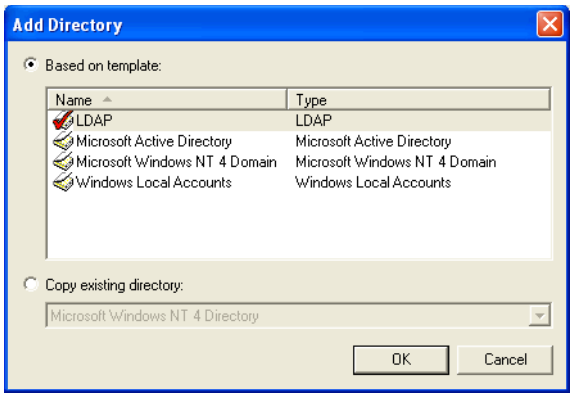
All directories with an e-mail attribute specified will be listed in the Linked account directories listing window on the Person E-mail Fields form in the Cardholder Options folder.

Directories Form Procedures

Use the following procedures on this form.

Add a Directory

1. From the ***Administration*** menu, select ***Directories***.
2. On the Directories form, click [Add]. The Add Directory window opens.



3. Do one of the following:
   - To create a directory that is based on a directory template:
     i. Select **Based on template**.
     ii. Click on the template you wish to use.
     iii. Click [OK].
   - To create a directory that is based on an existing directory:
     i. Select **Copy existing directory**.
     ii. In the drop-down list, select the existing directory that you wish to copy.
     iii. Click [OK].
4. In the **Name** field, type a name for the directory.
5. The sub-tabs available and the fields available on those sub-tabs differ depending on the type of directory that was selected. Select appropriate values for all available fields on all available sub-tabs.
6. Click [OK].

Modify a Directory

Note: After the **Type** has been selected for a directory, it cannot be modified.

1. From the ***Administration*** menu, select ***Directories***.
2. In the listing window on the Directories form, select the directory that you wish to change.
3. Click [Modify].
4. Make any desired changes in the fields on the sub-tabs.
5. Click [OK].

Delete a Directory

1. From the ***Administration*** menu, select ***Directories***.
2. In the listing window on the Directories form, select the directory that you wish to delete.
3. Click [Delete].
4. Click [OK].
   - If no accounts have been linked to the directory, it will be deleted without confirmation.
   - If accounts have been linked to the directory, a message will be displayed that says, “There are x user accounts and y cardholder accounts for this directory. If you delete this directory, these user and cardholder accounts will be unlinked. This operation cannot be undone. Are you sure you wish to continue?” Click [Yes]. The directory will then be deleted.

CHAPTER 14

Users Folder

The Users folder contains forms with which you can:

- Define users and their passwords.
- For each user, select a permission group for each portion of the software.
- Create permission groups, identifying levels of access to cardholder information fields.
- Create permission groups, identifying specific software features and devices that can be accessed.
- When segmentation is enabled, assign users multiple segments. It is recommended that Segment groups be used to accomplish this.
- Configure access levels that a user can assign.

The folder contains several forms: the Users form, Search form, System Permission Groups form, Cardholder Permission Groups form, Monitor Permission Groups form, Report Permission Groups form, and the Field/Page Permission Groups form.

Note: The availability of these forms is subject to licensing restrictions.

Selecting ***Users*** from the ***Administration*** menu, or by selecting the Users toolbar button.

Toolbar Shortcut

Users Form

The Users form contains six sub-tabs, the General sub-tab, Directory Accounts sub-tab, Internal Account sub-tab, Permission Groups sub-tab, Area Access Manager Levels sub-tab, and the Monitor Zone Assignment sub-tab. If segmentation is enabled, a seventh sub-tab, the Segment Access sub-tab is also present.

From the Users form, you can:

- Create usernames and passwords

- For a given username, choose a permission group for each user-related portion of the software (General, Directory Accounts, Internal Account, Permission Groups, Area Access Manager Levels, Monitor Zone Assignment, Segment Access if enabled, and User Replication Mode for Enterprise systems.)
- Disable user accounts

Users Form Common Fields

Listing window

Lists currently defined users. Each entry contains the user's name and ID, plus the user's System, Cardholder, Monitor, Replication mode, and Field/Page permission groups. Segmented systems also display the segment(s) that the user has access to.

If you see users named "New Trans User":

When you upgrade an OnGuard system, the upgrade process creates a user with the last name of "New Trans User" if the user transaction log contained a username that was not assigned to an existing user at the time of the upgrade. (Basically, this is a user account that was deleted. This is why it is recommended to disable a user account rather than delete it.) The user's internal account name is the username found in the user transaction log, the user's first name is the user's internal ID, and the user account is disabled by default. This user is created is so that user transaction reports will still print out the correct usernames for these old log entries.

Hide users whose access to this system is disabled

If selected, users whose access to OnGuard is disabled will not be displayed. If not selected, users whose access to OnGuard is disabled will be displayed.

Hide users that have been automatically created

If selected, users who have been automatically been created with the Bulk User tool will not be displayed. If not selected, users who have been automatically been created with the Bulk User tool will be displayed.

Add

Click on this button to add a user record.

Modify

Click on this button to change a selected user record.

Delete

Click on this button to delete a selected user record.

Help

Displays online help for this form.

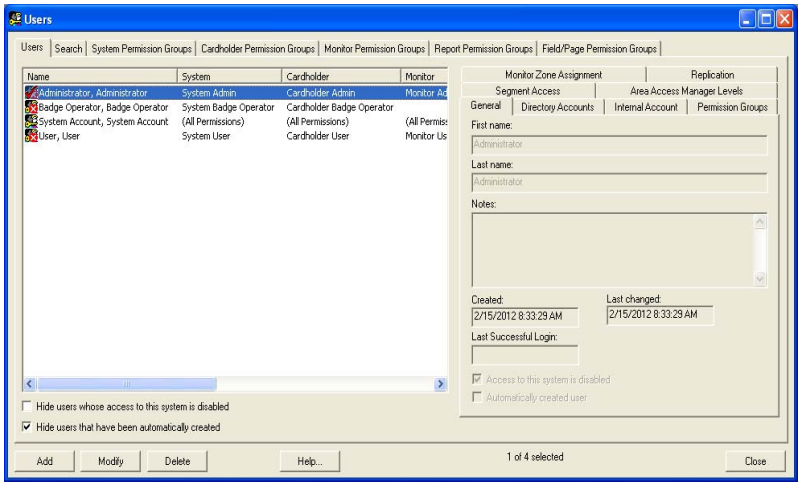
Mode

In view mode, indicates the record/selection count (such as "1 of 42 selected"). In modify mode, indicates the current operation, such as "Modify Mode."

Close

Closes the Users folder.

Users Form (General Sub-tab)



First name

Enter the user's first name as you want it to be displayed in the system. The **First name** and **Last name** fields are case-sensitive.

Last name

Enter the user's last name as you want it to be displayed in the system. The software is case-sensitive. This means that the capital and lowercase versions of a letter are considered two different letters. Therefore, the name "Smith" is not the same as the name "smith". This is why it is important to be consistent when entering names and other case-sensitive information.

Notes

This space allows you to add notes up to 2000 characters. These notes are optional and are NOT read only.

Created

This field is automatically filled and lists the date and time the record was created.

Last changed

This field is automatically filled and lists the date and time the record was changed.

Last Successful Login

Displays the date and time of the last successful login to the system.

Access to this system is disabled

This check box is only available for selection in add or modify mode. If selected, access to OnGuard for the selected user group is disabled.

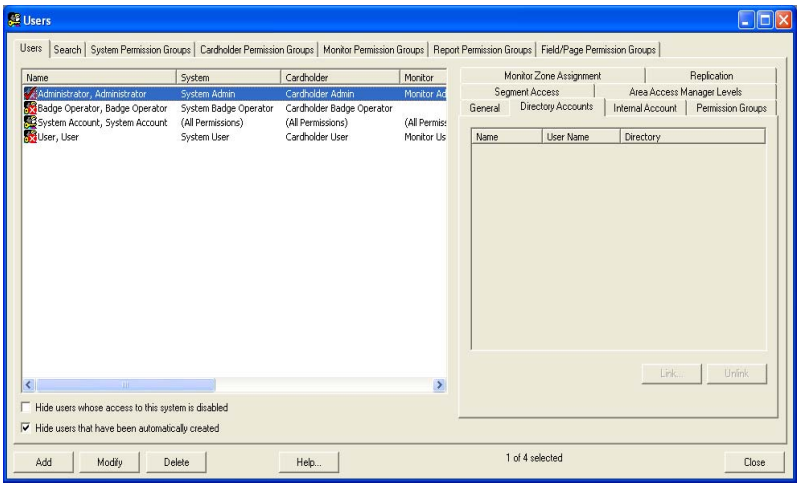
Automatically created user

A read-only field. If selected, that user has been automatically created using the Bulk User tool.

UL 1981

This check box is only available for systems with a UL 1981 license. Enable this check box to give the selected user UL 1981 security level.

Users Form (Directory Accounts Sub-tab)



Directory accounts listing window

Lists currently defined directory accounts in the application. Each entry contains the name, user name, and directory.

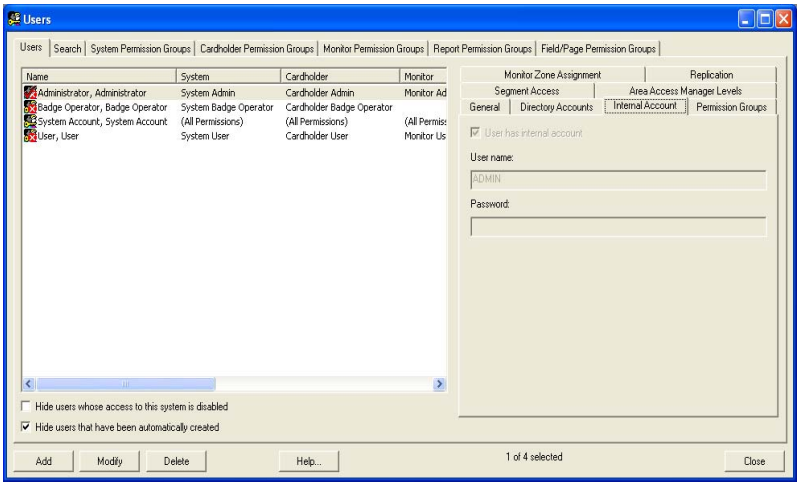
Link

This check box is only available for selection in add or modify mode. If clicked, the Select Account window is displayed, in which you can choose a directory and account to link to a user account.

Unlink

This check box is only available for selection in add or modify mode, and can only be clicked when a directory account-user account linkage is selected in the listing window. If clicked, the directory account and user account for the selected directory account-user account linkage are unlinked.

Users Form (Internal Account Sub-tab)



User has internal account

This check box is only available for selection in add or modify mode. If selected, indicates the user has an internal account. Enter values in the User name and Password fields, and then enter the password again in the Confirm password field. If not selected, indicates the user does not have an internal account. In this case, the **User name** and **Password** fields are not available.

User name

Enter a user name for this user. It's a good idea to choose a name that is meaningful to the user, such as the person's initials.

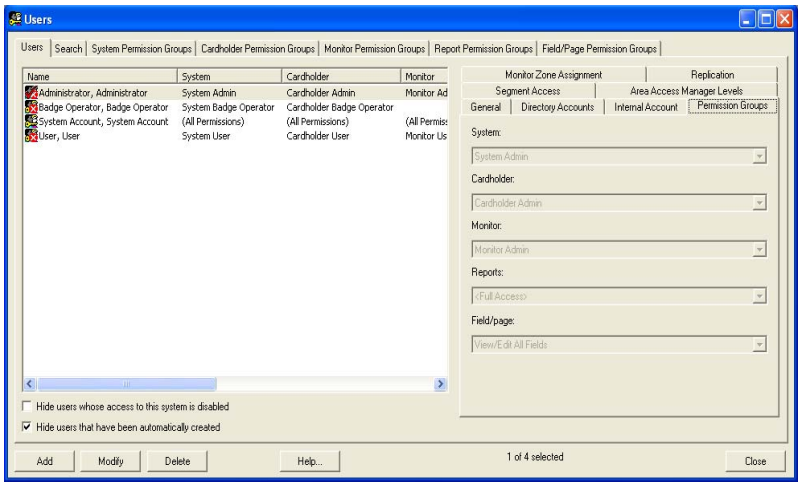
Password

Enter a password for this user.

Confirm password

This field is only available in the add or modify mode. Enter the password for confirmation.

Users Form (Permission Groups Sub-tab)



Note: If no permission group is selected for a particular permission, then the user will have no access to the functions managed by those permission groups.

System

Select a permission group for system administration functions. Choices are defined on the System Permission Groups form of this folder.

Cardholder

Select a permission group for cardholder record functions. Choices are defined on the Cardholder sub-tab of the Cardholder Permission Groups form in this folder.

Monitor

Select a permission group for alarm monitoring functions. Choices are defined on the Monitor Permission Groups form of this folder.

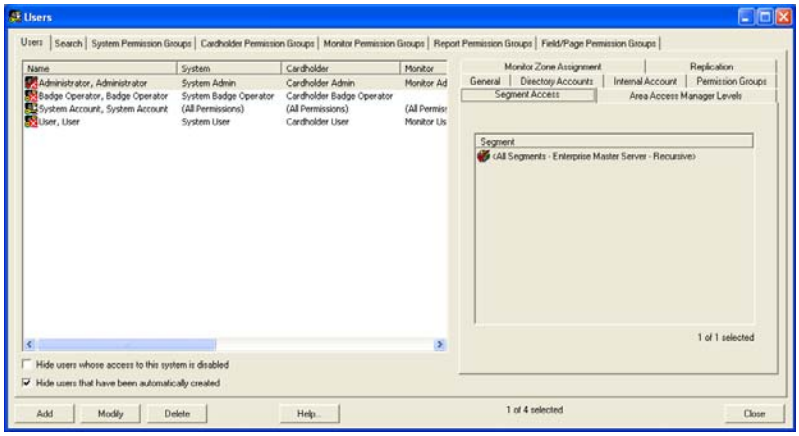
Reports

Select a permission group for report functions. Choices are defined on the Report Permission Groups form of this folder.

Field/page

Select a permission group for cardholder record viewing and editing functions. Choices are defined on the Field/Page Permission Groups form of this folder.

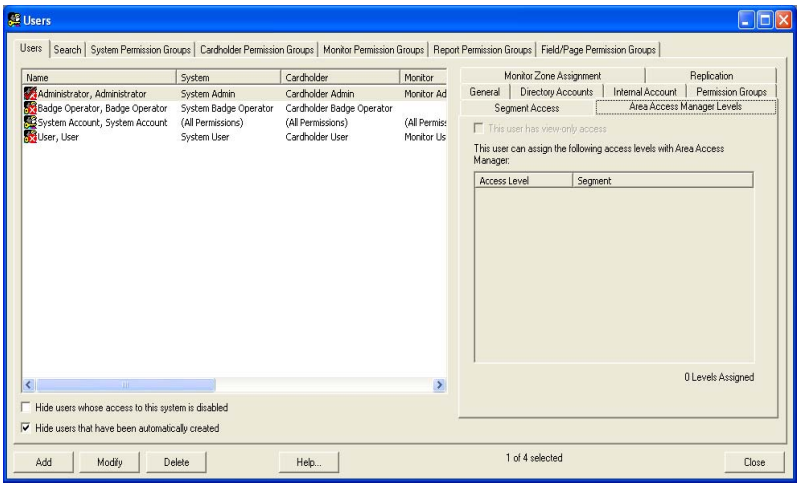
Users Form (Segment Access Sub-tab)



Segment listing window

Displays all segments that the user currently selected in the listing window on the Users form has access to.

Users Form (Area Access Manager Levels Sub-tab)



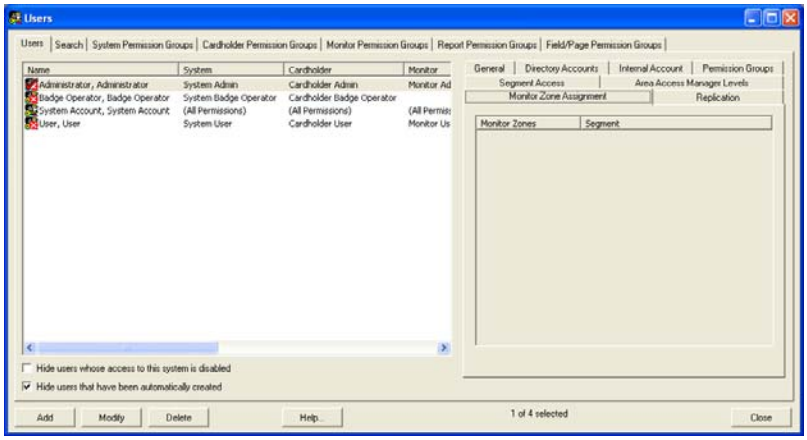
Area access levels listing window

In view mode, lists the access level (s) that the user who is currently selected in the listing window on the Users form has been assigned. In modify mode, lists all available access levels. In modify mode, you can select one or more access levels to assign to a selected user in this listing window.

This user has view-only access

If this option is selected, the user can only view access level assignments to people in Area Access Manager. They can not assign, remove, or edit access level activation dates. If this option is not selected for the user, then the user will have full access level assignment editing capabilities in Area Access Manager.

Users Form (Monitor Zone Assignment Sub-tab)

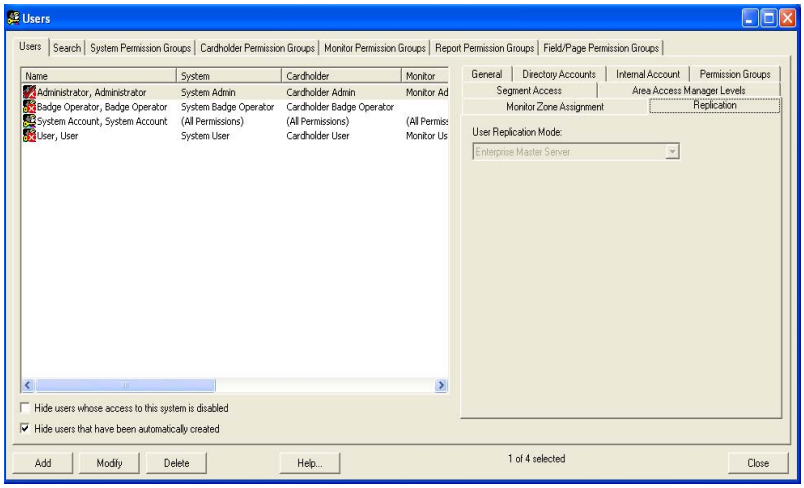


Monitor Zones listing window

In view mode, lists the monitor zone that the user who is currently selected in the listing window on the Users form has been assigned. In modify mode, lists all available monitor zones. In modify mode, you can select which monitor zone to assign to a selected user in the listing window.

User Form (Replication Sub-tab)

Note: The Replication sub-tab is only displayed for Enterprise systems.



User Replication Mode

Specify whether the user is replicated to the “Local Region Only” or “All Regions”.

Users Form Procedures

The following procedures can be performed on this form.

Add a User

1. From the ***Administration*** menu, select ***Users***.
2. On the Users form, click [Add].
3. On the General sub-tab, enter the user's first and last name.
4. On the Internal Account sub-tab, complete the following steps if the user is to have an internal account:
   a. Select the **User has internal account** check box.
   b. Enter the user name for the internal account.
   c. Enter the user's password. Enter the password a second time in the **Confirm password** field.
   d. Click [OK].
5. Click the Permission Groups sub-tab.
6. Choose system, cardholder, monitor, reports, and field/page permission groups for this user.

Notes: You must first define these permission groups on the System Permission Groups, Cardholder Permission Groups, Monitor Permission Groups, Report Permission Groups, and Field/Page Permission Groups sub-tabs of this folder.

If no permission group is selected for a particular permission, then the user will have no access to the functions managed by those permission groups.

7. Make selections on the Directory Accounts, Area Access Manager Levels, and Segment Access sub-tabs if desired.
8. On Enterprise systems, use the **User Replication Mode** drop-down on the Replication sub-tab to indicate whether the user should be replicated to the "Local Region Only" or "All Regions".
9. Click [OK].

Assign Access Level(s) to a User

1. From the ***Administration*** menu, select ***Users***.
2. In the listing window of the Users form, select the user record you want to assign an access level(s) to.
3. Click [Modify].
4. Click the Area Access Manager Levels sub-tab.
5. Click on the icon to the left of each access level you want to assign to the selected user. A checkmark appears on the icon of each selected access level.

Note: You must first define these access levels on the Access Levels form, which is opened by selecting the ***Access levels*** option from the ***Access Control*** menu.

6. Click [OK].

Assign a Monitor Zone to a User

1. From the ***Administration*** menu, select ***Users***.
2. In the listing window of the Users form, select the user record you want to assign a monitor zone to.
3. Click [Modify].
4. Click the Monitor Zone Assignment sub-tab.

5. Click on the icon to the left of the monitor zone you want to assign to the selected user. A checkmark appears on the icon of the selected monitor zone.

Note: You must first define monitor zones on the Monitor Zones form, which is opened by selecting the ***Monitor Zones*** option from the ***Monitoring*** menu.

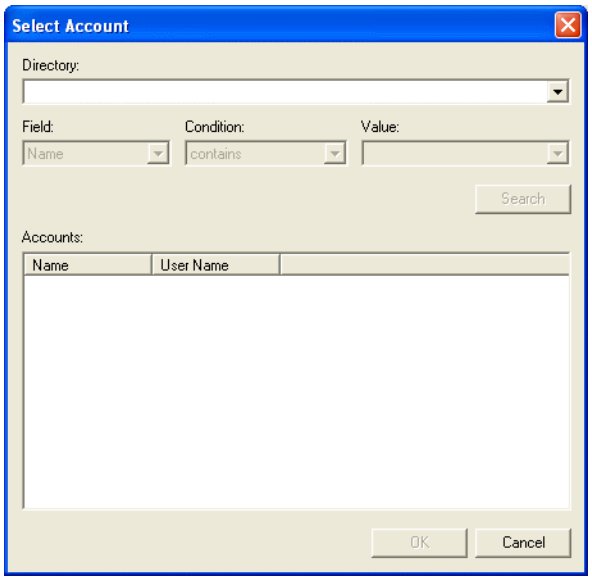
6. Click [OK].

Link a User Account to a Directory Account

1. From the ***Administration*** menu, select ***Users***.
2. On the Users form:
   - If you are adding a new user account, click [Add].
   - If you are modifying an existing user account, select existing user and click [Modify].
3. On the Directory Accounts sub-tab, click [Link].
4. The Select Account window open. In the Select Account window:
   a. In the **Directory** drop-down, select the directory you want to link to.
   b. In the **Field** drop-down select whether to search for a name or user name.
   c. In the **Condition** drop-down, select how the value will be related to the field. For example, a search where the **Field** selected is “Name”, the **Condition** selected is “contains”, and the **Value** specified is “Lake” will display all accounts where the name contains the word “Lake”, such as Lisa Lake.
   d. In the **Value** field, type or select a word you think may be in the user name or name. If you leave this field empty, all accounts for the selected directory will be displayed when the search is executed.

Note: To help you search, the **Value** field will contain different ways that the selected account may be expressed. For example, if the user account Lisa Lake is selected, the permutations listed might be “L. Lake”, “LISA”, “Lisa”, “Lisa L.”, “Lisa Lake”, “LL”, “Lake”, and “Lake, Lisa.”

   e. Click [Search].
   f. The accounts associated with the selected **Directory** will be displayed in the Accounts listing window.
      - If the account you want to link to is displayed, select it. Your window should look similar to the following:



- If the account you want to link to is not displayed, return to step d and select another **Value** to search for.

g. Click [OK].

h. Repeat steps 3 and 4 for each directory account you want to link to the selected user account.

5. Click [OK].

Unlink a User Account from a Directory Account

1. From the ***Administration*** menu, select ***Users***.
2. On the Users form in the listing window, select the user account you want to unlink a directory account from.
3. Click [Modify].
4. On the Directory Accounts sub-tab in the Directory accounts listing window, select the directory account-user account linkage you want to unlink.
5. Click [Unlink]. The directory account-user account linkage will be removed from the listing window.
6. Click [OK] to actually delete the directory account-user account linkage, or click [Cancel] to leave the directory account and user account linked.

Restrict User Access to Segments

An <All Segments> User with system administration privileges can choose the segment(s) to which a normal Segment User has access.

1. Select ***Users*** from the ***Administration*** menu. On the Users form, select the name of the user to be restricted.
2. Click [Modify].
3. Select the Segment Access sub-tab, if it is not already displayed.
4. A user can now belong to a single segment or to multiple segments. In the **Segment listing window**, select the segment(s) in which the user will work.
   - If you select the name of a segment (or segments), the person will be a regular <Segment User> and will be restricted to working within the specified segment.

- If you select the **<All Segments>** check box, the person will be an <All Segments> User, and can potentially (with proper permissions) view, add, modify, and delete records from all segments.

5. Click [OK] to save the changes, thereby restricting the user to the selected segments.

Modify User Information

1. From the ***Administration*** menu, select ***Users***.
2. In the listing window of the Users form, select the user record you want to change.
3. Click [Modify].
4. Make the changes you want to the fields. Changes can be made on any sub-tab.
5. Click [OK] to save the changes or [Cancel] to revert to the previously saved values.

Disable a User Account

1. From the ***Administration*** menu, select ***Users***.
2. In the listing window of the Users form, select the user account you want to disable.
3. Click [Modify].
4. On the General sub-tab, select the **Access to this system is disabled** check box.
5. Click [OK] to save the changes and disable the account or [Cancel] to revert to the previously saved values.

You can control whether disabled user accounts are shown in the Users listing window by selecting or deselecting the **Hide users who access to this system is disabled** check box.

Hide or Show Disabled User Accounts

1. From the ***Administration*** menu, select ***Users***.
2. To prevent user accounts from being displayed in the Users listing window, select the **Hide users whose access to this system is disabled** check box.
3. To show disabled user accounts in the Users listing window, deselect the **Hide users whose access to this system is disabled** check box.

Delete a User

IMPORTANT: Deleting a user is not recommended. Instead, disable the account. Disabling the account hides it by default from the users listing window. For more information refer to Disable a User Account on page 353 and Hide or Show Disabled User Accounts on page 353.

1. From the ***Administration*** menu, select ***Users***.
2. In the listing window of the Users form, select the user record you want to delete.
3. Click [Delete].
4. Click [OK].
5. Click [Yes] to confirm the deletion.

Search Form

This form is used to

- View users with specific permissions
- View users with specific group permissions
- Export the search results to a report

Search Type

Specifies the type of search for users:

- Permission Groups - Returns users that are assigned to the permission groups specified in the search criteria.
- Selected Permissions (AND) - Returns users that have permission granted for all permissions selected in the tree.
- Selected Permissions (OR) - Returns users that have permission granted for one of the permissions selected in the tree.

Search

After defining the search criteria, click this button to search for users with the selected permissions or permission groups.

Clear

Used to clear the current permission search selections.

Search results listing window

Lists users that meet the search criteria. Each entry contains the user's Name and ID, plus the System, Cardholder, Monitor, and Field/Page permission groups.

Export

Used to export the search results into a report in the Comma Delimited .csv file format.

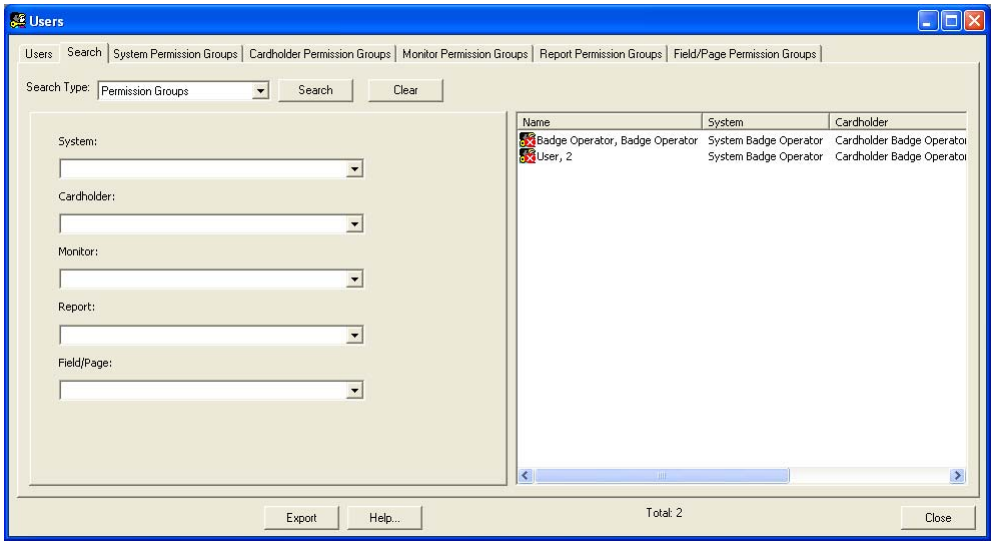
Help

Displays online help for this form.

Close

Closes the Users folder.

Search Form - Permission Groups Search Mode



When “Permission Groups” is the Search Type, you can search for users with common permission groups by selecting the permission group you want to search on from each of the permission group types, and then click [Search].

Note: If no selection is made in a group type, that group is ignored during the search.

When users are added, they are assigned to one or more permission groups. For more information, refer to Users Form (Permission Groups Sub-tab) on page 347.

System

Select the system permission group for which you want to find users.

Cardholder

Select the cardholder permission group for which you want to find users.

Monitor

Select the monitor permission group for which you want to find users.

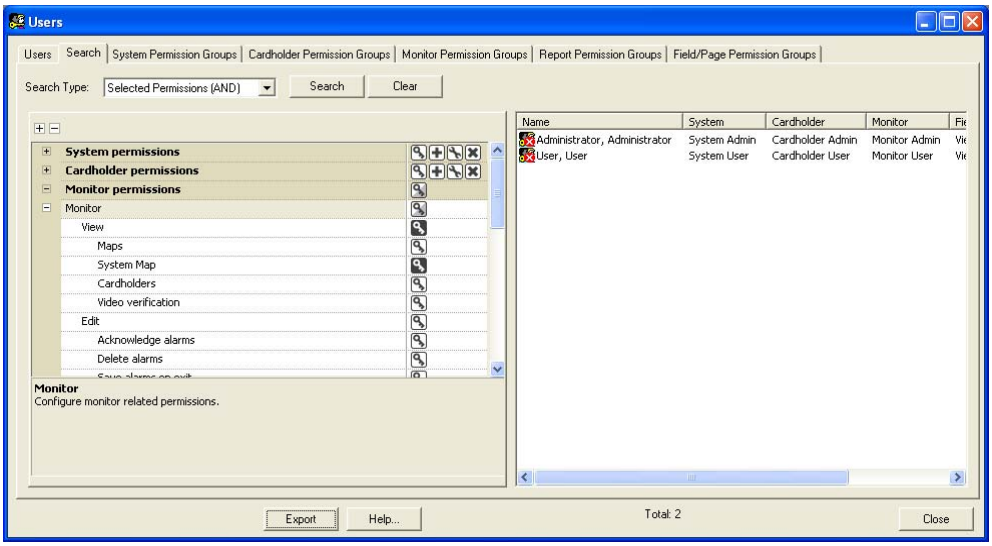
Report

Select the report permission group for which you want to find users.

Field/page

Select the field/page permission group for which you want to find users.

Search Form - Selected Permissions AND/OR Search Modes



Permission search tree

This is displayed when “Selected Permissions (AND)” or “Selected Permissions (OR)” is selected as the Search Type. Contains the combined permissions from the system, cardholder, and monitor permission groups. To search for users by permission, select the permission(s) from the tree, and then click [Search].

Note: Permission dependencies are not shown for the search function.

Permission Groups Tree

A permission groups tree is provided for configuring the permissions for System Permission Groups, Cardholder Permission Groups, Monitor Permission Groups, and Report Permission Groups. For more information, refer to the following topics:

- System Permission Groups Tree on page 362
- Cardholder Permission Groups Tree on page 365
- Monitor Permission Groups Tree on page 368
- Report Permission Groups Tree on page 372

Control Device Groups permissions are configured on the Control Device Groups form. For more information, refer to Monitor Permission Groups Form (Control Device Groups Sub-tab) on page 369.

Field/Page Permission Groups are configured on the Field/Page Permission Groups Form on page 374.

Configure User Permissions

You can configure the permissions individually or all permissions within a category. For example, changing the view/access rights at the **Users, directories, logical access** category level to “Permission granted” sets all permissions in that category to “Permission granted.” Categories are used to organize permissions by form and functionality.

In the tree, use the permission toggle buttons to modify the user's view/access, add, modify, or delete rights as described in the following tables:

Operate Permission Toggle Buttons at the Permission Level

Button		Status	Description
View/ Access		Permission granted	Allows the user to view a form or have access to an option on a form or menu, or run an application.
		Permission denied	The user is not allowed to view a form or access an option on a form.
		Not available	The user does not have rights to configure the View/Access option for this permission.
Add		Permission granted	Allows the user to add records on a form.
		Permission denied	The user is not allowed to add records a form.
		Not available	The user does not have rights to configure the Add option for this permission.
Modify		Permission granted	Allows the user to modify records on a form.
		Permission denied	The user is not allowed to modify records on a form.
		Not available	The user does not have rights to configure the Modify option for this permission.
Delete		Permission granted	Allows the user to delete records on a form.
		Permission denied	The user is not allowed to delete records on a form.
		Not available	The user does not have rights to configure the Delete option for this permission.

Operate Permission Toggle Buttons at the Category Level

Button		Status	Description
View/ Access		All permissions in category granted	Allows the user to view all forms and have access to all options belonging to the category.
		Some permissions in category granted	Allows the user to view at least one form or access at least one option belonging to the category.
		All permissions in category denied	The user is not allowed to view any form or access any option belonging to the category.
		Not available	The user does not have rights to configure the View/Access option for any permission belonging to the category.
Add		All permissions in category granted	Allows the user to add records on all forms belonging to the category.
		Some permissions in category granted	Allows the user to add records on at least one form belonging to the category.
		All permissions in category denied	The user is not allowed to add records on any form belonging to the category.
		Not available	The user does not have rights to configure the Add option for any permission belonging to the category.
Modify		All permissions in category granted	Allows the user to modify records on all forms belonging to the category.
		Some permissions in category granted	Allows the user to modify records on at least one form belonging to the category.
		All permissions in category denied	The user is not allowed to modify records on any form belonging to the category.
		Not available	The user does not have rights to configure the Modify option for any permission belonging to the category.

Operate Permission Toggle Buttons at the Category Level (Continued)

Button		Status	Description
Delete		All permissions in category granted	Allows the user to delete records on all forms belonging to the category.
		Some permissions in category granted	Allows the user to delete records on at least one form belonging to the category.
		All permissions in category denied	The user is not allowed to delete records on any form belonging to the category.
		Not available	The user does not have rights to configure the Delete option for any permission belonging to the category.

Keyboard Commands

Some actions in the permission trees have keyboard shortcuts associated with them.

Toggle the Permission Buttons

After you select a permission, press the following keys to toggle the permission buttons:

<1> = Toggles the View/Access permission button

<2> = Toggles the Add permission button

<3> = Toggles the Modify permission button

<4> = Toggles the Delete permission button

Navigate the Tree

Press the arrow Up and Down keys to navigate through the tree.

Search the Tree

First give the tree focus (click on the tree), and then press <Ctrl+F>. To continue through the search, press <F3>.

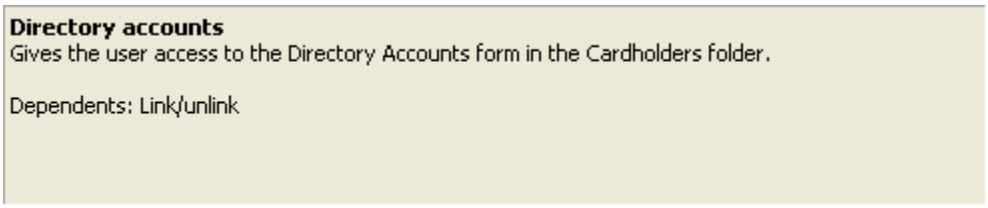
Expand All/Collapse All Permissions

Above each permission tree, click the Expand All button to expand all permissions or click the Collapse All button to collapse all permissions in the tree.

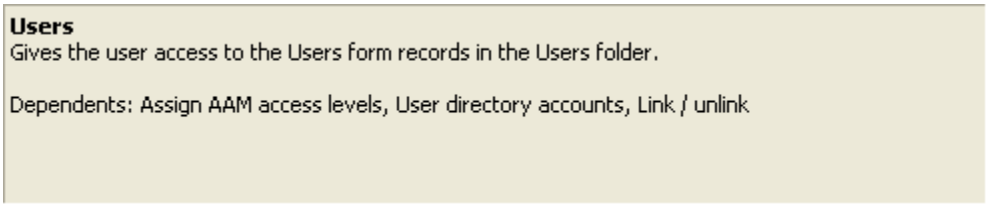
Optionally, press the arrow Left or Right keys on a category to expand or collapse the category's permissions.

Permission Dependencies

A description of the currently selected permission is displayed at the bottom the tree along with a list of permissions which depend on that permission:

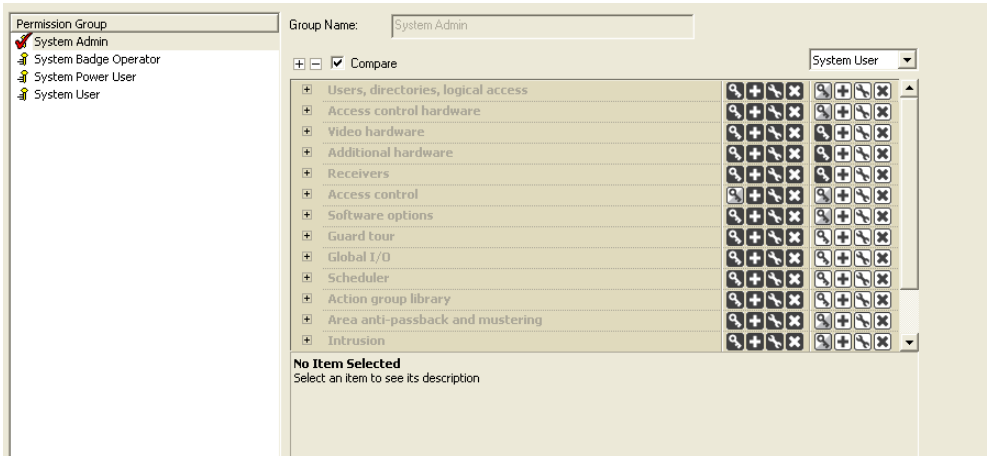


In this example, the user must be allowed to access the User directory accounts in order to link directory accounts to user accounts. (Link / unlink). Whereas, User directory accounts is dependent on access to the Users form:



Compare One Permission Group to Another

1. From the ***Administration*** menu, select ***Users***.
2. Click the System, Cardholder, Monitor, or Report Permission Groups tab.
3. In the Permission Group listing window, select the permission group you want to compare to.
4. Select the **Compare** check box. The comparison drop-down becomes available and an additional column of permissions is displayed on the right.



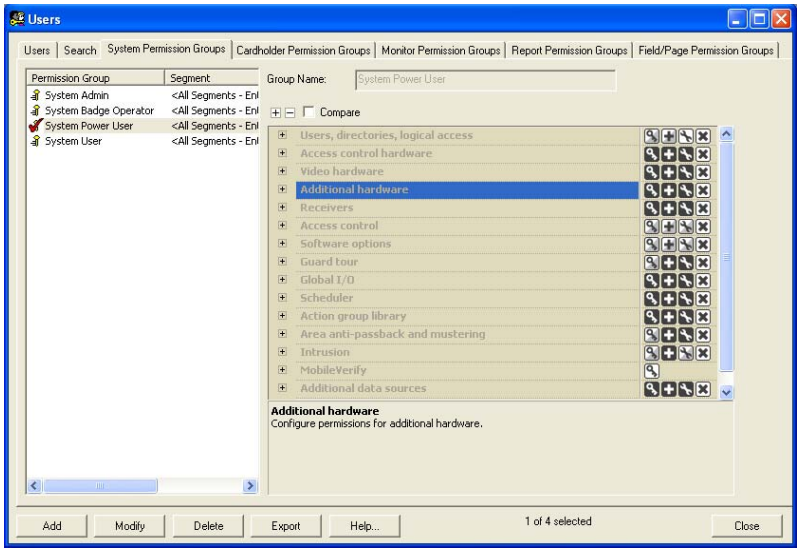
5. From the drop-down, choose the permission group you want to use to compare against the currently selected group (on the left).

Verify Permission Changes Using the Compare Function

1. From the ***Administration*** menu, select ***Users***.
2. Click the System, Cardholder, Monitor, or Report Permission Groups tab.

3. In the listing window, select the name of the permission group you want to update.
4. Click [Modify], and then make any required changes to the permissions.
5. Select the **Compare** check box, and then select the same permission group you are updating. You can compare your proposed changes in the left column to the existing permissions:
6. Click [OK] to confirm your changes or Cancel.

System Permission Groups Form



This form is used to create permission groups, each of which contains a set of abilities to access system functions.

Listing window

Lists currently defined system permission groups. To select an entry, click on the entry or its icon. Only one entry may be selected at a time. The record for the currently selected entry is displayed in the System Permission Groups tree. For more information, refer to System Permission Groups Tree on page 362.

Group Name

In view mode, displays the name of the system permission group that is currently selected in the listing window of the Users form. In modify mode, you can enter a name for a system permission group. The permission group contains all of the permissions configured in the tree.

Compare

Select to compare the permissions of the currently selected permission group against those of another group. From the drop-down, select the permission group you want to compare. An additional column will be displayed with the permissions configured for the comparable group. Deselect the **Compare** check box to close the “compare” mode.

Note: You can also compare a permission group against itself. This would be done in modify mode if you need to compare the existing permission settings to your changes before confirming them. For more information, refer to Verify Permission Changes Using the Compare Function on page 360.

Add
Used to add a system permission group.

Modify
Used to change a system permission group.

Delete
Used to delete a system permission group.

Export
Used to export the system permission settings into a report in the Comma Delimited .csv format. If **Compare** is selected, exports the compared permission groups information.

Help
Displays online help for this form.

Close
Closes the Users folder.

System Permission Groups Tree

The system permission groups tree is organized by category which is generally based on system forms. For example, permissions to add, modify, or delete records on the Access panels forms belongs to the **Access control hardware** category.

Other permission types allow the user to access options on a form or menu as well as run an application. Examples of these permissions include **Local I/O** and **Programming** (in the **Access control hardware** category) which allow the user to access and program the Local I/O features.

Dependencies

A description of the currently selected permission is displayed at the bottom of the tree followed by any dependencies (when you modify a system permission, it might depend on the setting of another permission). For example:

- The user must be allowed to View/Access the Groups forms (Mask groups, in the **Access control hardware** category) in order to access the Local I/O features, and the user must have access to the Local I/O features in order to Program the Local I/O features.
- **Change threat level setting to anything** and **Change threat level setting to higher than default only** (in the **MobileVerify** category) cannot have the same rights.

For more information, refer to Permission Dependencies on page 360.

Note: If you have an Enterprise system, **Distributed ID** (allows the user to access the Distributed ID/Mobile Configuration group of forms) is replaced by **Enterprise** (allows the user to access the Enterprise group of forms). This permission belongs to the **Software options** category.

System Permission Groups Form Procedures

The following procedures can be performed on this form.

Add a System Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the System Permission Groups tab.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this permission group will be assigned to.
   b. Click [OK].
5. In the **Group Name** field, type a unique, descriptive name for this permission group.
6. In the System Permission Group tree, configure the permissions that correspond to the capabilities you want to include in this permission group. For more information, refer to Configure User Permissions on page 356.
7. Click [OK].

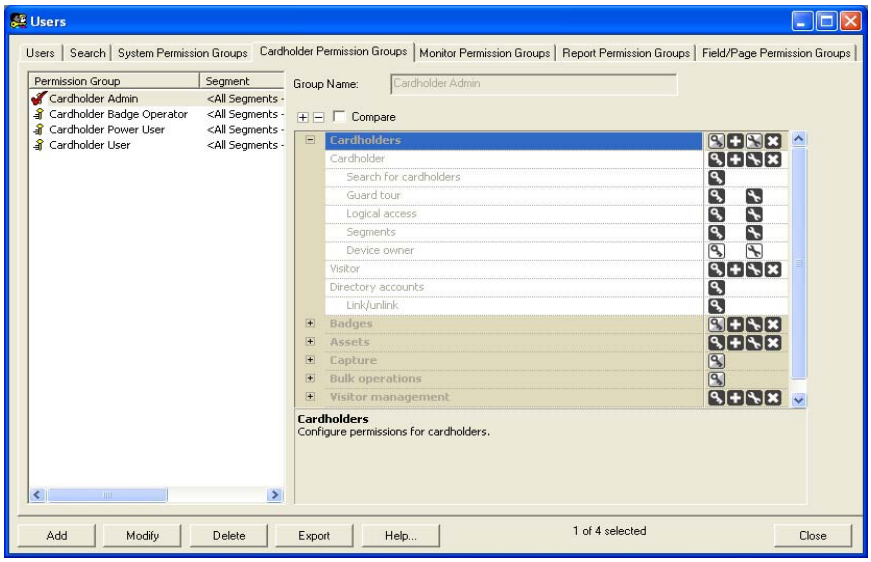
Modify a System Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the System Permission Groups tab.
3. In the listing window, select the name of the permission group you want to change.
4. Click [Modify].
5. In the System Permission Group tree, change the permissions as required. For more information, refer to Configure User Permissions on page 356.
6. Click [OK] to save the changes or [Cancel] to revert to the previously saved values.
7. A warning message will be displayed, reporting that modifying the permission group will affect all users who are assigned to that group. Click [Yes] to confirm or [No] to cancel.

Delete a System Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the System Permission Groups tab.
3. In the listing window, select the name of the permission group you want to delete.
4. Click [Delete].
5. Click [OK].
6. Click [Yes] to confirm the deletion.

Cardholder Permission Groups Form



This form is used to create permission groups, each of which contains a set of abilities to access cardholder record functions.

Note: The Badge Types folder, badge printing, and multimedia capture are subject to licensing restrictions. Although you may be able to change permissions for those features here, they will have no effect unless you have the appropriate license.

Listing window

Lists currently defined cardholder permission groups. The record for the currently selected entry is displayed in the Cardholder Permission Groups tree. For more information, refer to Cardholder Permission Groups Tree on page 365.

Group Name

In view mode, displays the name of the cardholder permission group that is currently selected in the listing window of the Users form. In modify mode, you can enter a name for a cardholder permission group. The permission group will contain all of the permissions settings configured in the tree.

Compare

Select to compare the permissions of the currently selected permission group against those of another group. From the drop-down, select the permission group you want to compare. An additional column will be displayed with the permissions configured for the comparable group. Deselect the **Compare** check box to close the “compare” mode.

Note: You can also compare a permission group against itself. This would be done in modify mode if you need to compare the existing permission settings to your changes before confirming them. For more information, refer to Verify Permission Changes Using the Compare Function on page 360.

Add

Used to add a cardholder permission group.

Modify
Used to change a cardholder permission group.

Delete
Used to delete a cardholder permission group.

Export
Used to export the cardholder permission settings into a report in the Comma Delimited .csv format. If **Compare** is selected, exports the compared permission groups information.

Help
Displays online Help for this form.

Close
Closes the Users folder.

Cardholder Permission Groups Tree

The cardholder permission groups tree is organized by *category* which is generally based on the forms in the Cardholder folder. For example, the permissions to add, modify, or delete records on the Badge form belong to the Badge category.

Other permission types allow the user to view a form or access options on a form or menu. Examples of such permissions include searching for cardholders, using or modifying the guard tour features, linking or unlinking directory accounts to users, and using or modifying the logical access features.

Dependencies

When you modify cardholder group permissions, some might be dependent on other permissions. For example:

- The user must have permission to **View/Access** the Cardholders form in order to add, modify, or delete records on the Visit form since an associated cardholder is required.
- Users with the **Deactivate settings** permission granted should also have the **List Builder Delete** permission (located on the System Permission Groups > Software Options category). **Deactivate settings** belongs to the Cardholder Permissions > Badges category.

For more information, refer to Permission Dependencies on page 360.

IMPORTANT: Do not grant the user permission to **Destroy all cardholder data** unless the user understands the impact of such an action. This permission belongs to the Bulk operations category.

Notes: **Bulk change replication** is available for Enterprise systems only. This permission allows the user to select **Change Cardholder Replication** from the ***Cardholder > Bulk*** menu.

Segment permissions are applicable to segmented systems only.

The **Print badges** permission and the Capture category are subject to licensing restrictions.

Cardholder Permission Groups Form Procedures

The following procedures can be performed on this form.

Add a Cardholder Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Cardholder Permission Groups tab.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this permission group will be assigned to.
   b. Click [OK].
5. In the **Group Name** field, type a unique, descriptive name for this permission group.
6. In the Cardholder permission tree, configure the permissions that correspond to the capabilities you want to include in this permission group. For more information, refer to Configure User Permissions on page 356.
7. Click [OK].

Modify a Cardholder Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Cardholder Permission Groups tab.
3. In the listing window, select the name of the permission group you want to change.
4. Click [Modify].
5. In the Cardholder Permission Groups tree, change the permissions as required.
6. Click [OK] to save the changes or [Cancel] to revert to the previously saved values.
7. A warning message will be displayed, reporting that modifying the permission group will affect all users who are assigned to that group. Click [Yes] to confirm or click [No] to cancel.

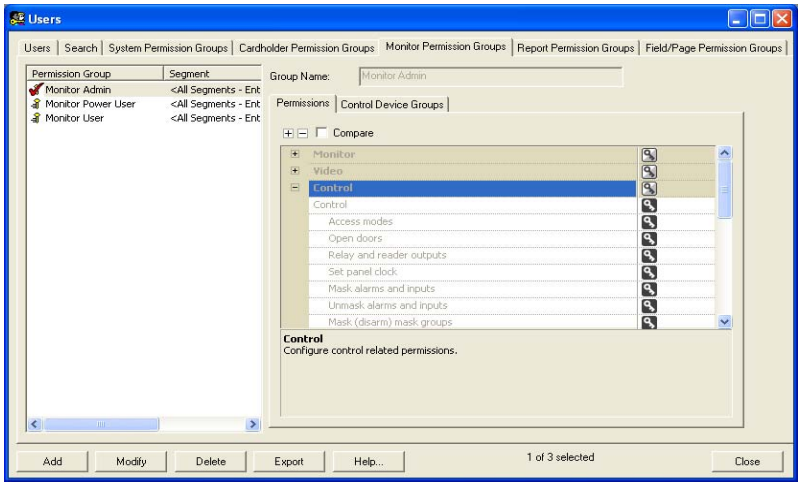
Delete a Cardholder Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Cardholder Permission Groups tab.
3. In the listing window, select the name of the permission group you want to delete.
4. Click [Delete].
5. Click [OK].
6. Click [Yes] to confirm the deletion.

Monitor Permission Groups Form

This form is used to create permission groups, each of which contains a set of abilities to access alarm monitoring functions and/or device groups.

Monitor Permission Groups Form (Permissions Sub-tab)



Listing window

Lists currently defined monitor permission groups. The record for the currently selected entry is displayed in the Monitor Permission Groups tree. For more information, refer to Monitor Permission Groups Tree on page 368.

Group Name

In view mode, displays the name of the monitor permission group that is currently selected in the listing window of the Users form. In modify mode, you can enter a name for a monitor permission group. The permission group will contain all of the permissions settings configured in the tree.

Compare

Select to compare the permissions of the currently selected permission group against those of another group. From the drop-down, select the permission group you want to compare. An additional column will be displayed with the permissions configured for the comparable group. Deselect the **Compare** check box to close the “compare” mode.

Note: You can also compare a permission group against itself. This would be done in modify mode if you need to compare the existing permission settings to your changes before confirming them. For more information, refer to Verify Permission Changes Using the Compare Function on page 360.

Add

Used to add a Monitor permission group.

Modify

Used to change a Monitor permission group.

Delete

Used to delete a Monitor permission group.

Export

Used to export the monitor permission settings into a report in the Comma Delimited .csv format. If **Compare** is selected, exports the compared permission groups information.

Help
Displays online help for this form.

Close
Closes the Users folder.

Monitor Permission Groups Tree

The Monitor permission groups tree is organized by category allowing you to easily locate and configure the Monitor, Video, and Control related permissions. Unlike the other permission groups trees, the Monitor permission groups tree does not contain permissions to add, modify, or delete records on forms but rather offers permissions that allow the user to edit, view, trace, and control operations in Alarm Monitoring.

For example, in the Monitor category, **Disabling of automatic alarm display options** allows the user to turn off the following Options menu items:

- Automatic Map Display
- Automatic Cardholder Display
- Automatic Video Verification
- Automatic Visual Notification
- Automatic Live Video Display

Other permissions allow the user to view live or recorded video and export video as well as use the camera PTZ functionality.

Dependencies

When you modify monitor group permissions, some might be dependent on other permissions. For example: The permission **Video > Export video** is only applicable if **Recorded video** is allowed. For more information, refer to Permission Dependencies on page 360.

A user transaction is generated each time the Video Export dialog is opened, regardless of how many times the video is actually exported or if not exported at all.

A user transaction is not generated when the VideoViewer Browser-based Client is used to export video. If you want to disable video export from the VideoViewer Browser-based Client for all users, add the following line to the **C:\Inetpub\wwwroot\Lnl.OG.Web\Preferences.js** file on the computer running the Web Application Server:

```
var g_lnl_enable_export_video = false;
```

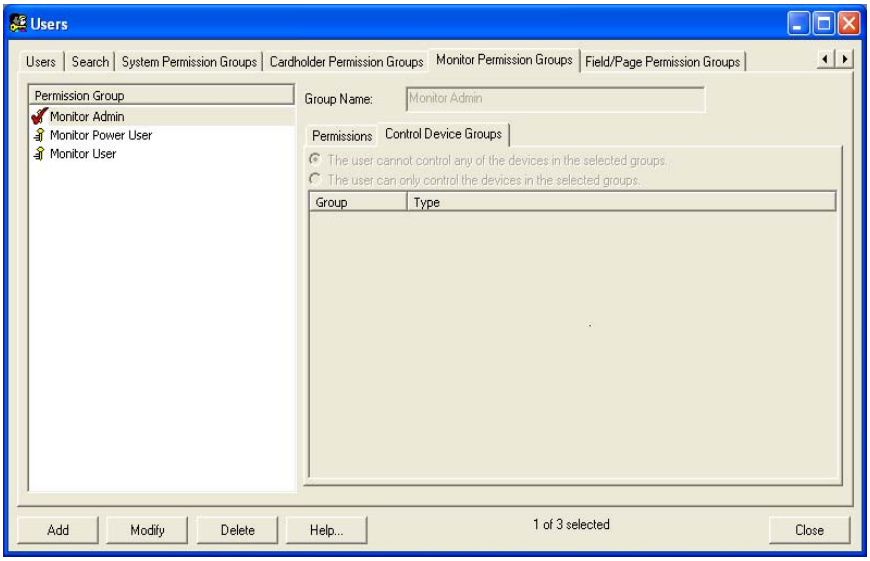
Monitor > Windows logout upon monitoring logout must always be denied for the SA account. SA can always log out of the application without logging out of Windows.

In order to limit the number of channels in the **Video > Max channel count** permission, toggle the View/Access button to “Permission granted” and then type a value in the field next to the button.

For permissions with associated fields, you can use a keyboard command to move the cursor over to the field value. After you select the permission, press <2> and then type the value.

For the **Control > Camera PTZ** permission, toggle the View/Access button to “Permission granted” and then type a value in field next to the button. This field specifies the priority level of the user. Since only one person can control a PTZ camera at a time, a user with higher priority can take over PTZ control of a camera from someone who has lower priority. Configure the PTZ priority level from 1 - 255 (where 1 is the lowest priority and 255 is the highest).

Monitor Permission Groups Form (Control Device Groups Sub-tab)



The user cannot control any of the devices in the selected groups.

Select this radio button if you want to deny a permission group access to a group of devices. The groups selected in the group listing window will be unavailable to the permission group.

The user can only control the devices in the selected groups.

Select this radio button if you want to grant a permission group access to a group of devices. Only groups selected in the group listing window will be available to the permission group.

Group listing window

Displays the name and type of groups available in the system and the segment they belong to. Group devices are configured in the Groups folder, Device Groups form.

Monitor Permission Groups Form Procedures

The following procedures can be performed on this form.

Add a Monitor Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Monitor Permission Groups tab.
3. Select the Permissions sub-tab.
4. Click [Add].
5. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this permission group will be assigned to.
   b. Click [OK].
6. In the **Group Name** field, type a unique, descriptive name for this permission group.
7. On the Permissions sub-tab, configure permissions that correspond to the capabilities you want to include in this permission group. For more information, refer to Configure User Permissions on page 356.
8. On the Control Device Groups sub-tab:
   a. Select the check box(es) to configure the permissions.
   b. Select the device groups you want to grant or deny the permission group access to.
9. Click [OK].

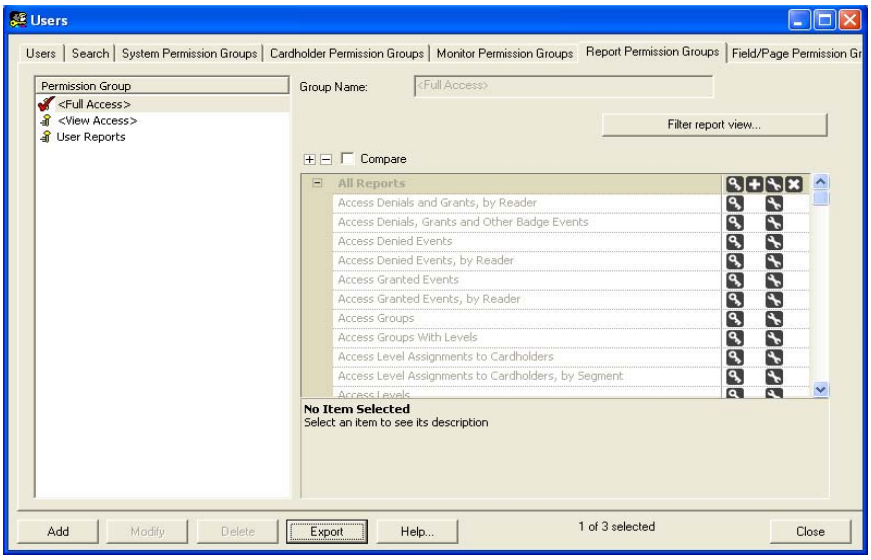
Modify a Monitor Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Select the Monitor Permission Groups tab.
3. Select the Permissions sub-tab.
4. In the listing window, select the permission group you want to change.
5. Click [Modify].
6. On the Permissions or Control Device Groups sub-tab, change the permissions and device groups selections as required.
7. Click [OK] to save the changes or [Cancel] to revert to the previously saved values.
8. A warning message will be displayed, reporting that modifying the permission group will affect all users who are assigned to that group. Click [Yes] to confirm or click [No] to cancel.

Delete a Monitor Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Monitor Permission Groups tab.
3. In the listing window, select the name of the permission group you want to delete.
4. Click [Delete].
5. Click [OK].
6. Click [Yes] to confirm deletion.464

Report Permission Groups Form



This form is used to create permission groups, each of which contains a set of abilities to preview, add, modify, and delete reports.

Listing window

Lists currently defined report permission groups. The record for the currently selected entry is displayed in the Report Permission Groups tree. For more information, refer to Report Permission Groups Tree on page 372.

Two report permission groups are provided by default:

- Full Access–Allows the user to preview, modify, add, or delete reports.
- View Access–Allows the user to preview reports, but cannot delete, modify, or add reports.

For any other report permissions, the user must create custom report permission groups.

Note: The Full Access and View Access report permission groups update automatically when users create new reports. Therefore, users with Full Access or View Access report permissions will receive full or view access to custom reports automatically. Users must add new reports to custom report permission groups manually.

Group Name

In view mode, displays the name of the report permission group that is currently selected in the listing window of the Users form. In modify mode, you can enter a name for a report permission group. The permission group will contain all of the permissions settings configured in the tree.

Filter Report View

Click this button to display the Report View Filter window from where you can choose the types of reports you wish to view. For more information, refer to Report View Filter Window on page 207.

Compare

Select to compare the permissions of the currently selected permission group against those of another group. From the drop-down, select the permission group you want to compare. An

additional column will be displayed with the permissions configured for the comparable group. Deselect the **Compare** check box to close the “compare” mode.

Note: You can also compare a permission group against itself. This would be done in modify mode if you need to compare the existing permission settings to your changes before confirming them. For more information, refer to Verify Permission Changes Using the Compare Function on page 360.

Add
Used to add a report permission group.

Modify
Used to change a report permission group.

Delete
Used to delete a report permission group.

Export
Used to export the report permission settings into a report in the Comma Delimited .csv format. If **Compare** is selected, exports the compared permission groups information.

Help
Displays online Help for this form.

Close
Closes the Users folder.

Report Permission Groups Tree

The report permission groups tree lists all available reports. You can provide preview and modify permissions separately for each report. Add and delete permissions are set globally for all reports.

To find a report in the tree, press <Ctrl><F> to open the Find dialog. Press <F3> to find the next occurrence of your search term.

Note: On Enterprise systems, all servers follow the permissions from the report permission groups. Therefore, if a user has permission to modify a report on a Regional Server, then the user will also have permission to modify the report on the Master Server (and vice versa).

Dependencies

When you modify report group permissions, some might be dependent on other permissions. For example:

- The user must have permission to **View/Access** at least one report in order to add, modify, or delete reports.
- The user must have permission to **Modify** at least one report in order to modify or delete reports.
- Users with **Delete** permissions can only delete the reports that they can modify.

For more information, refer to Permission Dependencies on page 360.

Report Permission Groups Form Procedures

The following procedures can be performed on this form.

Add a Report Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Report Permission Groups tab.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership dialog opens. Select the segment that this permission group will be assigned to.
   b. Click [OK].
5. In the **Group Name** field, type a unique, descriptive name for this permission group.
6. In the Report Permission Groups tree, configure the permissions that correspond to the capabilities you want to include in this permission group. For more information, refer to Configure User Permissions on page 356.
7. Click [OK].

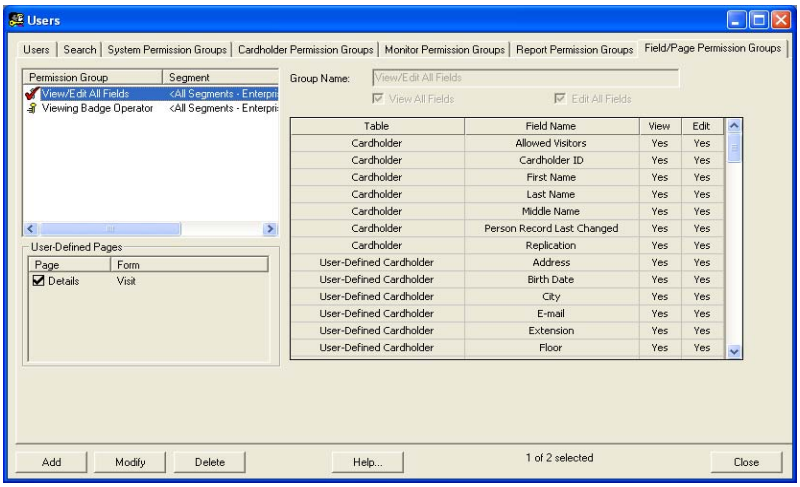
Modify a Report Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Report Permission Groups tab.
3. In the listing window, select the name of the permission group you want to change.
4. Click [Modify].
5. In the Report Permission Groups tree, change the permissions as required.
6. Click [OK] to save the changes or [Cancel] to revert to the previously saved values.
7. A warning message is displayed, reporting that modifying the permission group will affect all users who are assigned to that group. Click [Yes] to confirm, or click [No] to cancel.

Delete a Report Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Report Permission Groups tab.
3. In the listing window, select the name of the permission group you want to delete.
4. Click [Delete].
5. Click [OK].
6. Click [Yes] to confirm the deletion.

Field/Page Permission Groups Form



This form is used to create field permission groups, identifying levels of access to cardholder information fields.

Listing window

Lists currently defined field/page permission groups.

User-Defined Pages

Select the user-defined pages you want the permission group to be able to view/edit in the Cardholders, Visits and/or Visitors folders.

Note: The Details page is considered a user-defined page that is automatically created. You can create (define) other pages in FormsDesigner. The pages you define display as forms in their respective Cardholders, Visits, or Visitors folder. The Details form opens in the Visits folder.

Group Name

Specifies the name of a field/page permission group.

View All Fields

Select this box to allow a user having this permission group to view all cardholder database fields.

Edit All Fields

Select this box to allow a user who has this permission group to change all cardholder database fields.

Field table

Lists all the fields you can set permissions for. This includes user-defined and default fields.

Each row entry in the table contains the Table, Field Name, View, and Edit fields.

Note: In order to use Visitor Management, the Viewing Badge Operator permission group must be changed. For the Cardholder, the **Allowed Visitors** property must be changed to **Yes** in the **View** column.

Table

(column in the field table) Indicates the name of the table the field belongs to.

Field Name
(column in the field table) Indicates the name of the field. This is not the actual field name used by the database. It is the "friendly" or "logical" name, as defined using the FormsDesigner application.

View
(column in the field table) Indicates whether this field is visible to a user who has this permission group. Modify this field to enable/disable the permission to view the specified field. This applies only to a specific field on a page/form. Therefore, you can allow a permission group to view specific fields on a page or view entire pages. To enable a permission group to view the entire page/form, you must enable each field on the page/form.

Note: Double-clicking an individual cell toggles it between "Yes" or "No." Clicking the column head will change all fields in that column to the same value as it toggles between "Yes" or "No."

Edit
(column in the field table) Indicates whether a user with this permission group can change this field. Toggle this field to enable/disable the permission to modify the specified field. This applies only to a specific field on a page/form. Therefore, you can allow a permission group to modify specific fields on a page or modify entire pages. To enable a permission group to modify the entire page/form, you must enable each field on the page/form.

Note: Double-clicking an individual cell toggles it between "Yes" or "No." Clicking the column head will change all fields in that column to the same value as it toggles between "Yes" or "No."

Add
Used to create a field/page permission group containing the selected capabilities.

Modify
Used to change a field/page permission group.

Delete
Used to delete a field/page permission group.

Mode
In view mode, indicates the record/selection count (such as "1 of 42 selected"). In modify mode, indicates the current operation, such as "Modify Mode."

Close
Closes the Users folder.

Field/Page Permission Groups Form Procedures

The following procedures can be performed on this form.

Add a Field/Page Viewing Permission Group

1. From the ***Administration*** menu, select ***Users***.

2. Click the Field/Page Permission Groups tab.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this permission group will be assigned to.
   b. Click [OK].
5. In the **Group Name** field, type a unique, descriptive name for this permission group.
6. Scroll through the field table. For each field, choose a value in the View column (to indicate whether the field will be displayed on the corresponding form(s)).

   For each field in the table, choose a value in the Edit column (to indicate whether the user will be able to change the field on the corresponding form(s)). Here are some tips:

   - Double-click on a "Yes" value to change it to "No", and vice-versa. Some values will change automatically. For example, if you set the View value for a particular field to "No", the Edit value for that field automatically changes to "No". This is because you can't change the information in a field if you can't even see the field.
   - Select the **View All Fields** check box to change all values in the View column to "Yes"
   - Select the **Edit All Fields** check box to change all values in the Edit column to "Yes". All values in the View column will also be changed to "Yes", because a field must be displayed on the form in order for you to edit it.
   - Double-click on a column heading (View or Edit) to change all values in that column
   - Double-click on a Field Name to change both of the corresponding View and Edit values to "Yes" or "No".
7. Click [OK] to save the selected capabilities as the specified field restrictions permission group.

Modify a Field/Page Viewing Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Field/Page Permission Groups tab.
3. In the listing window, select the name of the permission group you want to change.
4. Click [Modify].
5. Make the changes you want to the field table.
6. Click [OK] to save the changes or [Cancel] to revert to the previously saved values.
7. A warning message will be displayed, telling you that modifying the permission group will affect all users who are assigned to that group. Click [Yes] to continue with the modification or click [No] to cancel.

Delete a Field/Page Viewing Permission Group

1. From the ***Administration*** menu, select ***Users***.
2. Click the Field/Page Permission Groups tab.
3. In the listing window, select the name of the permission group you want to delete.
4. Click [Delete].
5. Click [OK].
6. Click [Yes] to confirm the deletion.

CHAPTER 15

Workstations Folder

The Workstations folder contains forms with which you can:

- Add, modify, and delete workstations
- Configure options for activity printers, CCTV controllers, and video capture devices
- Add, modify, and delete encoders/scanners

The folder contains two forms, the Workstations form and the Encoders/Scanners form.

This folder is displayed by selecting ***Workstations*** from the ***Administration*** menu, or by selecting the Workstations toolbar button.

Toolbar Shortcut

Workstations Form

The following table identifies the fields common to the sub-tabs on the Workstations form.

Listing window
Lists previously defined workstations.

Name
The name of an existing or planned workstation. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse
Opens a Browse for Computer form, from which you can select a workstation.

Add
Adds a workstation record.

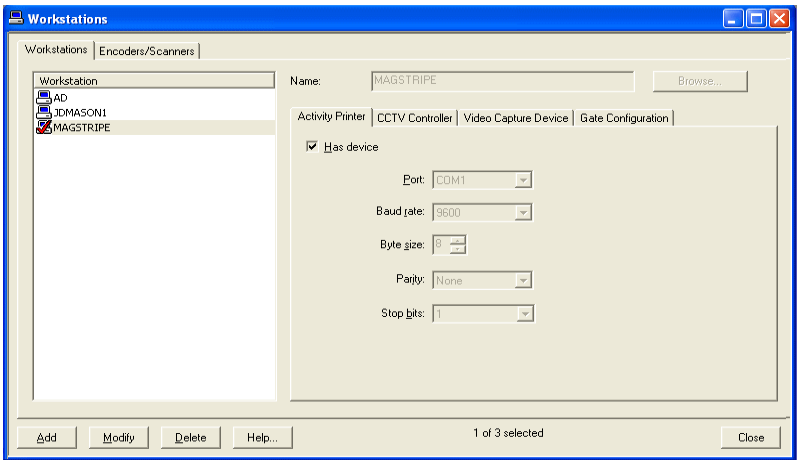
Modify
Changes a workstation record.

Delete
Deletes a workstation record.

Help
Displays online help for this topic.

Close
Closes the Workstations folder.

Workstations Form (Activity Printer Sub-tab)



Has device
If selected, indicates that this workstation has an attached printer for alarms. To print an alarm you must select the **Print Alarm** check box on the Alarm Definitions form of the Alarm Configuration folder. This field activates the **Port**, **Baud rate**, **Byte size**, **Parity**, and **Stop bits** fields.

Port
The communication port the activity printer attaches to.

Baud rate
The rate, in bits per second (bps), data is transferred. This field applies only if the port for the activity printer is a COM port (RS-232 serial port).

Byte size
The byte size of data transferred via the activity printer's communication port.

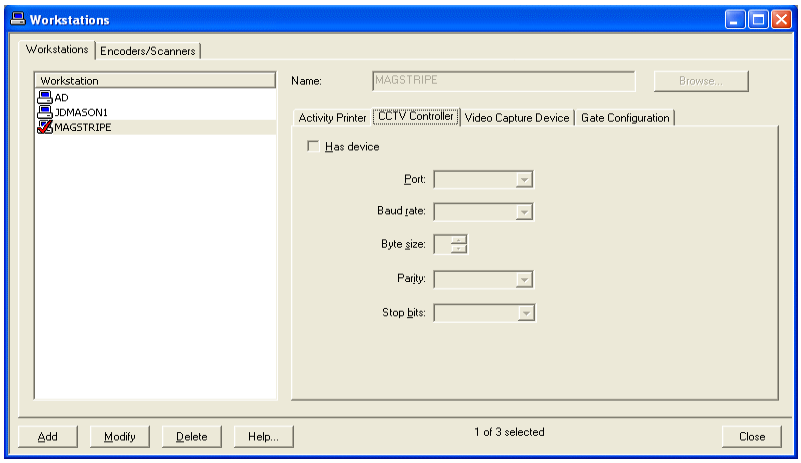
This field applies only if the port for the activity printer is a COM port (RS-232 serial port).

Parity
Parity is a technique of checking data when it is moved or transmitted, to confirm that data was not lost or written over. This field applies only if the port for the activity printer is a COM port (RS-232 serial port).

Stop bits

The number of stop bits used in data transmission via the activity printer's communication port. Each block of data sent/received during asynchronous data transmission (communication between the workstation and encoder/scanner device at irregular intervals) is prefixed with 1 start bit and suffixed with 1, 1.5 or 2 stop bits. The *start bit* lets the receiving end know when a new block has started. The *stop bit(s)* indicate the end of the block. This field applies only if the port for the activity printer is a COM port (RS-232 serial port).

Workstations Form (CCTV Controller Sub-tab)



Has device

If selected, indicates that this workstation has an attached CCTV controller to which CCTV command strings will be sent during alarm monitoring. This field activates the **Port**, **Baud rate**, **Byte size**, **Parity** and **Stop bits** fields.

Note that CCTV instructions (configured in the Alarm Configuration folder) are automatically sent to CCTV controllers when their associated workstations (monitoring stations) receive alarms containing CCTV instructions.

Port

The communication port the CCTV controller attaches to.

Baud rate

The rate, in bits per second (bps), data is transferred via the CCTV controller's communication port. This field applies only if the port for the activity printer is a COM port (RS-232 serial port).

Byte size

The byte size of data transferred via the CCTV controller's communication port. This field applies only if the Port for the activity printer is a COM port (RS-232 serial port).

Parity

Parity is a technique of checking data when it is moved or transmitted, to confirm that data was not lost or written over. This field applies only if the port for the activity printer is a COM port (RS-232 serial port).

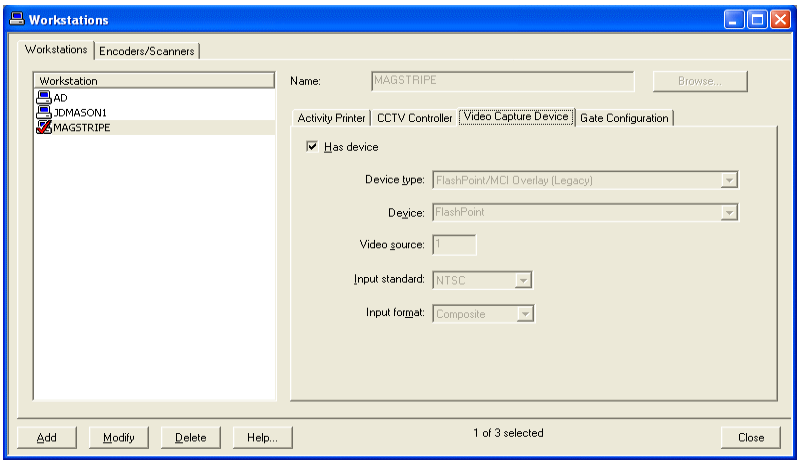
Stop bits

The number of stop bits used in data transmission via the CCTV controller's communication port. Each block of data sent/received during asynchronous data transmission (communication between

the workstation and encoder/scanner device at irregular intervals) is prefixed with 1 start bit and suffixed with 1, 1.5 or 2 stop bits. The *start bit* lets the receiving end know when a new block has started. The *stop bit(s*) indicate the end of the block. This field applies only if the Port for the activity printer is a COM port (RS-232 serial port).

Workstations Form (Video Capture Device Sub-tab)

This view displays when "FlashPoint/MCI Overlay (Legacy)" is selected in the **Device type** drop-down list. The same fields display when "WDM (Windows Driver Model)" is selected in the **Device type** drop-down list except for the **Input format** field, which does not display.



Has device

If selected, indicates that this workstation contains a video board. This field activates the **Device type**, **Device**, **Video source**, **Input standard**, and **Input format** fields.

Device type

The type of video board you are using.

Device

The name of the video board you are using.

Video source

The video connector number.

Input standard

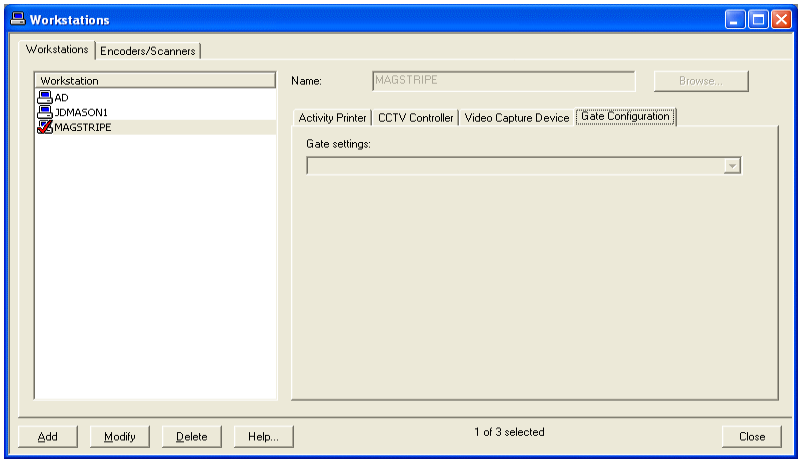
The video input standard used. The options available change depending on the **device type** and **device** selected. Two commonly selected options are:

- NTSC (U.S.A. standard)
- PAL (European standard)

Input Format

The video interface standard. The options available change depending on the **device type** and **device** selected. If the **Device type** selected is "WDM (Windows Driver Model)", this field is not displayed.

Workstations Form (Gate Configuration Sub-tab)



Gate setting

The name of the gate associated with the selected workstation. Gates are configured on the Gates form in the MobileVerify folder. For more information, refer to Chapter 20: MobileVerify Folder on page 485. For detailed information on MobileVerify and the Gate Configuration sub-tab, refer to the MobileVerify User Guide.

Workstations Form Procedures

Use the following procedures on this form.

Add a Workstation Entry

1. From the ***Administration*** menu, select ***Workstations***. The Workstations folder opens.
2. Click [Add].
3. In the **Name** field, enter the name of the workstation.
4. If you do not wish to configure an activity printer, skip this step. Otherwise, select the Activity Printer sub-tab.
   a. Select the **Has device** check box.
   b. Select the options that are appropriate for the printer.
5. If you do not wish to configure a CCTV controller, skip this step. Otherwise, select the CCTV Controller sub-tab.
   a. Select the **Has device** check box.
   b. Select the options that are appropriate for the CCTV controller.
6. If you do not wish to configure a video capture device, skip this step. Otherwise, select the Video Capture Device sub-tab.
   a. Select the **Has device** check box.
   b. Select the options that are appropriate for the video capture device.
7. If you do not wish to configure gates, skip this step. Otherwise:
   a. Select the Gate Configuration sub-tab.

b. From the **Gate settings** drop-down list, select the name of the gate that you want associated with this workstation.

8. Click [OK].

Modify a Workstation Entry

1. In the listing window, click the name of the workstation you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields. Changes can be made on any sub-tab.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Workstation Entry

1. In the listing window, click the name of the workstation you wish to delete.
2. Click [Delete].
3. Click [OK]. The workstation entry will be deleted without confirmation.

Encoders/Scanners Form

The Encoders/Scanners form is used to define encoder/scanner settings. The configuration fields on this form change depending on your selection in the **Device Type** drop-down list.

OnGuard currently supports the following device types:

- CSS Scanner - a device allows to import cardholder data from a driver's license or passport. Connected through a USB port, it will be dynamically discovered on the workstation.
- Digion24 (iCLASS) - an inline contactless encoder. This device should be configured the same as the HID iClass encoder. In addition the Baud rate must be set to 38400.
- Digion24 (MIFARE) - used to encode any application that resides on a MIFARE smart card or DESFire (TWIC 1.02 Data Model). In addition, the Baud rate must be set to 9600.
- GemEasyLink680S/GemEasyAccess332 - a MIFARE encoder for V-Smart and SmartID (MIFARE) applications. This unit works as either a standalone unit or inline with printing hardware.
- HID iCLASS - an internal iCLASS reader/encoder that allows you to encode iCLASS credentials from OnGuard software. It can also be used to import cardholder data from iCLASS credentials for the following applications: GSC (iCLASS), HandKey (iCLASS), HID Access Control (iCLASS), Lenel (iCLASS), IrisAccess (iCLASS), and V-Smart (iCLASS).
- ID-Check Terminal - a scanner that allows you to import cardholder data from a driver's license or military ID. This unit must be configured through the OnGuard software.
- Magstripe Swipe Reader/Writer (Model 712) - a standalone encoder for magnetic cards. This is a discontinued model that OnGuard supports.
- Magstripe Swipe Reader/Writer (Model 722) - a standalone encoder for magnetic cards. This is a discontinued model that OnGuard supports.
- MSR206 - a standalone magstripe encoder for GemEasyLink680S/GemEasyAccess332 applications. The MSR206 is also built into the Magicard Rio and Tango printers.
- OmniKey (iCLASS) - a standalone OMNIKEY 5321 reader/encoder for the Lenel (iCLASS) application.

- PC/SC Encoder - a Personal Computer/Smart Card encoder that supports International Standards Organization (ISO 7816) and PC/SC standards.
- MIFARE Pegoda Contactless Smart Card Reader (MF EV700) - an encoder connected through a USB port. On the encoding station, the drivers and DESFire reader hardware must be installed from the Supplemental Materials disc, after which it will be available for selection in the OnGuard software. To find the drivers navigate to \Credential Center Device Drivers\Integrated Engineering Drivers on the Supplemental Materials disc.
- Serial Encoder - any smart chip encoder that supports standard R-232 encoding protocols. The serial encoder is used with Credential Agent smart card applications.
- SmartID/Pro - SmartID/Pro is an USB interfaced encoder that supports DESFire card technology.
- V-Smart (iCLASS) - a Bioscrypt device used to capture fingerprint templates and encode V-Smart biometric applications on iCLASS credentials, when it is connected to an enrollment station. The V-Smart (iCLASS) also serves as an access control device for iCLASS credentials encoded with Bioscrypt V-Smart applications, when connected to a Lenel panel.
- V-Smart (MIFARE) - a Bioscrypt device used to capture fingerprint templates and encode V-Smart biometric applications on MIFARE credentials, when it is connected to an enrollment station. The V-Smart (MIFARE) also serves as an access control device for MIFARE credentials encoded with Bioscrypt V-Smart applications, when connected to a Lenel panel.

Encoding Prerequisites

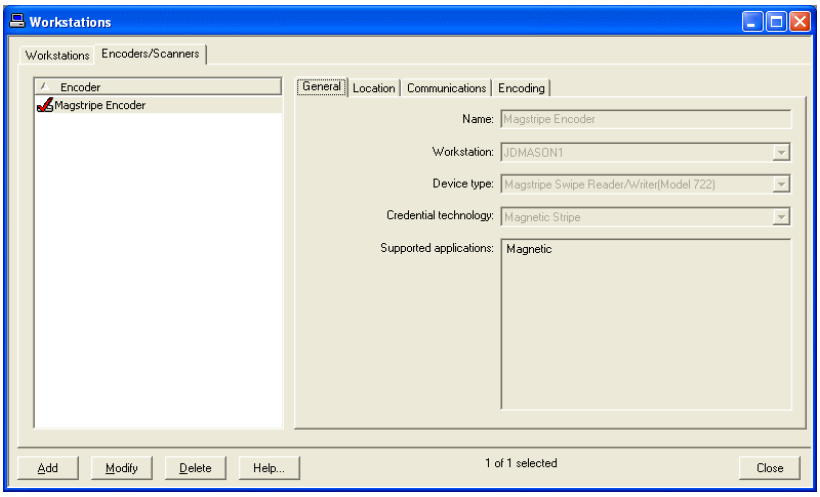
Several steps must occur in OnGuard to properly encode a magnetic, Wiegand, or smart card. Each step occurs in a different folder in the OnGuard application.

1. In the Workstations folder > Encoding form, configure an inline or standalone encoder/scanner.

Note: You do not need to configure USB encoders/scanners (e.g. MIFARE Pegoda contactless smart card reader) in OnGuard applications. Simply install the drivers and attach the hardware to the workstation. This does not apply to the ScanShell 800/1000.

2. In the Card Formats folder, create a card format that will contain data to be encoded on a badge.
3. In the Badge Types folder > Encoding form, assign an encoding format to a badge type. In other words, assign a card format to be encoded on a badge of a specific type.
4. In the Cardholders folder, add a cardholder or visitor record to the database.
5. In Multimedia Capture, capture the cardholder/visitor’s photo, signature, and/or biometric data.
6. In the Cardholders folder, encode the badge.

Encoders/Scanners Form (General Sub-tab)



Encoder listing window

Lists previously defined encoders/scanners.

Name

A descriptive name for the encoder/scanner.

Workstation

The workstation the encoder/scanner attaches to. Only workstations that have been configured on the Workstations form display in the drop-down list.

Device type

The type of encoder/scanner. The remaining fields on this form change, depending on the device type you choose.

Credential technology

The type of card that will be scanned/encoded by the specified device. This field automatically populates. However, if a device handles multiple types of cards, you can select the credential technology from the drop-down list.

Supported applications

The applications supported by the specified device. This field automatically populates.

Add

Adds an encoder/scanner record.

Modify

Modifies an encoder/scanner record.

Delete

Deletes an encoder/scanner record.

Help

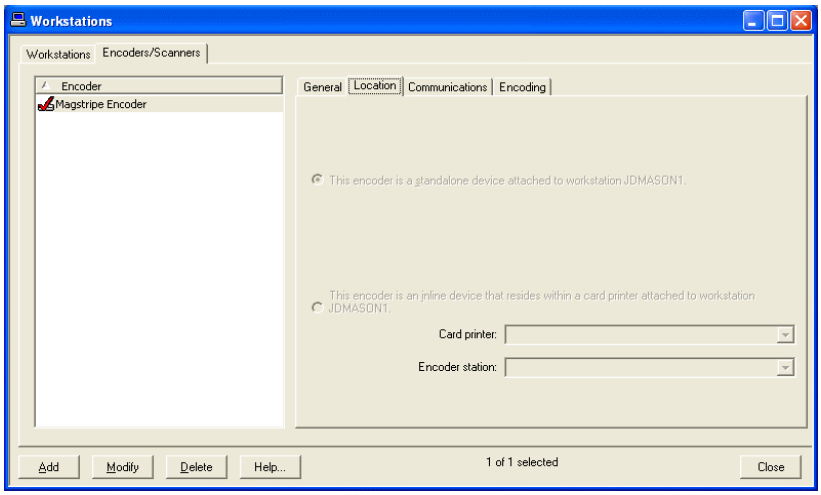
Displays online help for this form.

Close

Closes the Workstations folder.

Encoders/Scanners Form (Location Sub-tab)

The Location sub-tab displays two radio buttons that identify the encoding device as either being a standalone device or an inline device that resides within a card printer.



This encoder is a standalone device attached to this workstation.

This radio button is automatically selected by default. Select this radio button if the encoder is a standalone device and attached to the workstation (listed on the General sub-tab).

This encoder is an inline device that resides within a card printer attached to this workstation.

This field is reserved for configuring inline smart chip encoders with a future OnGuard version.

Card printer

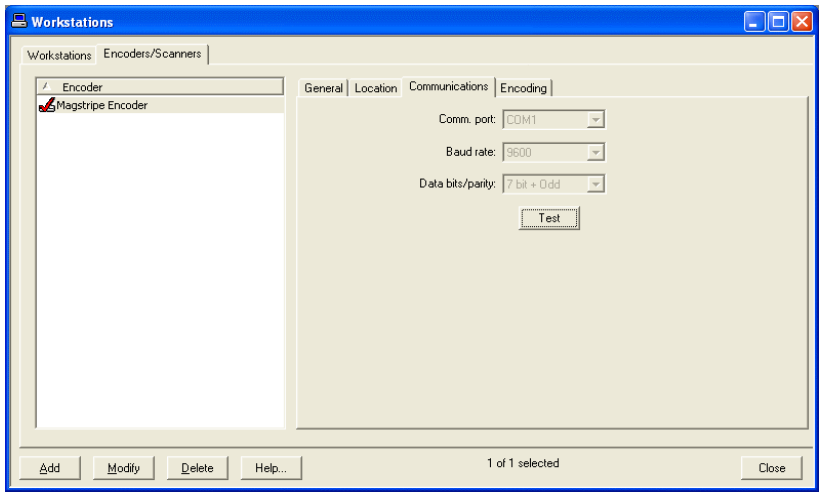
This field is reserved for configuring inline smart chip encoders with a future OnGuard version.

Encoder station

This field is reserved for configuring inline smart chip encoders with a future OnGuard version.

Encoders/Scanners Form (Communications Sub-tab)

Different fields display on the Communications sub-tab depending on the device type selected on the General sub-tab.



Comm. port

The communication port on the workstation that the encoder/scanner connects to.

Baud rate

This field automatically populates with the default setting for the specified device type. However, you can select the rate, in bits per second (bps) that data is transferred. The baud rate entered must match the fixed baud rate on the hardware.

Data bits

This field automatically populates with the default setting for the specified device type. However, you can select the number of bits of data transmitted per character, between the workstation and the encoder/scanner. This does not include start, stop or parity bits. The *data bits* value indicates whether the encoder/scanner uses the standard ASCII character set, with 7 bits forming each of 128 different characters, or the extended ASCII character set, with 8 bits forming each of 256 different characters.

Parity

This field automatically populates with the default setting for the specified device type. However, you can select the parity of data transferred via the encoder/scanner's communication port. *Parity* is a technique of checking data when it is moved or transmitted, to confirm that data was not lost or written over.

Stop bits

This field automatically populates with the default setting for the specified device type. However, you can select the stop bits if necessary. Each block of data sent/received during asynchronous data transmission (communication between the workstation and encoder/scanner device at irregular intervals) is prefixed with 1 start bit and suffixed with 1, 1.5 or 2 stop bits. The *start bit* lets the receiving end know when a new block has started. The *stop bit(s)* indicate the end of the block.

Data bits/parity

The parity of data transferred via the encoder/scanner's communication port. Choices include:

- **7 bit + Odd** - For each character transmitted between the workstation and the encoder there will be seven bits of data plus one bit for odd parity information. The value of the parity bit will be zero if there are an odd number of data bits that have a value of one. Otherwise, the parity bit will have a value of one.

- **7 bit + Even** - For each character transmitted between the workstation and the encoder there will be seven bits of data plus one bit for even parity information. The value of the parity bit will be zero if there are an even number of data bits that have a value of one. Otherwise, the parity bit will have a value of one.
- **7 bit + Mark** - For each character transmitted between the workstation and the encoder there will be seven bits of data plus one “mark” bit (a bit value of one).
- **7 bit + Space** - For each character transmitted between the workstation and the encoder there will be seven bits of data plus one “space” bit (a bit value of zero).
- **8 bit + None** - For each character transmitted between the workstation and the encoder there will be eight bits of data and no parity information.

IP Address

Enter the Internet Protocol (IP) address for the device. An IP address consists of four numbers, each in the range of 0 through 255. The IP address entered in this field must match the IP address programmed for the device.

Sound Volume

This setting is used to control the volume of voice messages for the IrisAccess iCAM. Select **Mute** to silence the voice messages.

Test

Verifies the encoder can communicate with the workstation.

Test Connection

(Applies when configuring IrisAccess iCAM) Verifies the device can communicate with the workstation.

PC/SC Device

The Personal Computer/Smart Card (PC/SC) for the specified encoder. *PC/SC* is a standard for communicating with smart cards connected to Windows machines. PC/SC enables smart cards, smart card encoders/readers, and computers made by different manufacturers to work together. If the PC/SC device is located on a remote workstation, you can add the encoder name to OnGuard using any computer but you must go to the remote workstation to complete the encoder configuration (populate the Communications sub-tab).

Flow control

This field automatically populates with the default setting for the specified device type. However, you can select the flow control if necessary. The *flow control* manages the flow of data between computers, devices or nodes in a network. Choices include:

- **Xon /Xoff** - uses two nominated characters to signal to the remote end that it should stop or start transmitting data.
- **Hardware** - allows either of the two stations to signal whether it is ready to receive more data, or if the other station should pause until the receiver is done processing the incoming data.
- **None** - no flow control applied.

SmartID/Pro device

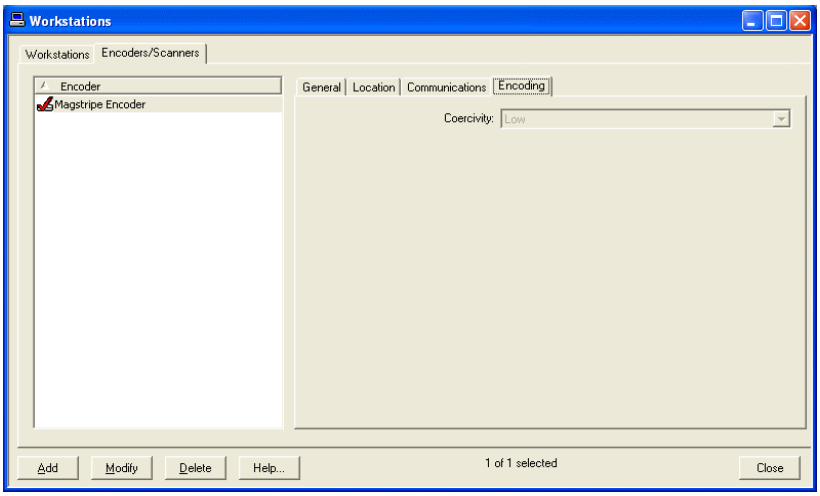
This field lists all the SmartID/Pro devices attached to the workstation. Select the one that best suits your needs.

OMNIKEY Device

If the selected **Device type** on the **General** tab is **OmniKey (iCLASS)**, then the **OMNIKEY device** field becomes available on the **Communications** tab. If multiple OmniKey encoders are connected to the workstation, then select each device in the **Encoder** listing window and choose the appropriate device from the **OMNIKEY device** drop-down.

Encoders/Scanners Form (Encoding Sub-tab)

The Encoding sub-tab displays when you are working with either the Magstripe Swipe Reader/Writer (Model 722) or MSR206 encoder/scanner. Otherwise, this sub-tab does not display.



Coercivity

Coercivity is the intensity of the magnetic field needed to reduce the magnetization of material after it has reached saturation. Select a high coercivity when possible. Magnetic stripes encoded with low coercivity are not as strongly magnetized and are more susceptible to magnetic fields.

Encoders/Scanners Form Procedures

Use the following procedures on this form.

Configure an Inline or Standalone Encoder/Scanner

1. From the ***Administration*** menu, select ***Workstations***. The Workstations folder opens.
2. Select the Encoders/Scanners tab and click [Add].
3. On the General sub-tab:
   a. In the **Name** field, enter a descriptive name for the encoder/scanner.
   b. From the **Workstation** drop-down list, select the workstation this encoder/scanner attaches to.
   c. Select a **Device type**.
   d. The **Credential technology** field automatically populates. However, if more than one technology is supported, you can select a different technology from the drop-down list.
4. On the Location sub-tab, verify the default settings are correct. If necessary, select the card printer and encoder station from the drop-down lists.

5. On the Communications sub-tab, populate the different fields that display.
6. If the Encoding sub-tab displays, select the coercivity.
7. Click [OK].

Modify an Encoder/Scanner Entry

1. In the listing window, select the name of the encoder/scanner you wish to change.
2. Click [Modify].
3. Change any field on any sub-tab.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an Encoder/Scanner Entry

1. In the listing window, select the name of the encoder/scanner you wish to delete.
2. Click [Delete].
3. Click [OK].

CHAPTER 16

System Options Folder

The System Options folder contains forms with which you can:

- Identify the peripheral devices that are attached to OnGuard workstations
- Configure hardware limits for the maximum number of holidays, timezones, access levels, badge length, elevator floors
- Configure the maximum access level assignments per badge
- Reset anti-passback status
- Configure the maximum number of templates and security levels of biometric readers
- Configure asset mode
- Configure the extended held open times and pre-alarm time
- Configure the default recipients that will receive E-mail notifications for visits
- Extend access level options (e.g. enable escorting)
- Configure the system to generate an alarm when a device enters a “runaway” state
- Configure controller encryption
- Specify the VideoViewer URL to enable launch from Alarm Monitoring

The folder contains different forms, depending on whether segmentation has been enabled.

- In a non-segmented system, the System Options folder contains the General System Options form as well as the General Assets Options, Web Applications, Hardware Settings, Anti-Passback, Biometrics, User Commands, Visits, Access Levels/Assets, and Controller Encryption forms.
- In a segmented system, the System Options folder contains only the General System Options, General Asset Options, and Web Applications forms. The Hardware Settings, Anti-Passback, Biometrics, User Commands, Visits, Access Levels/Assets, and Controller Encryption forms appear as sub-tabs on the Segments form in the Segments folder when segmentation is enabled.

This form displays when you select ***System Options*** from the ***Administration*** menu, or select the System Options toolbar button.

Toolbar Shortcut

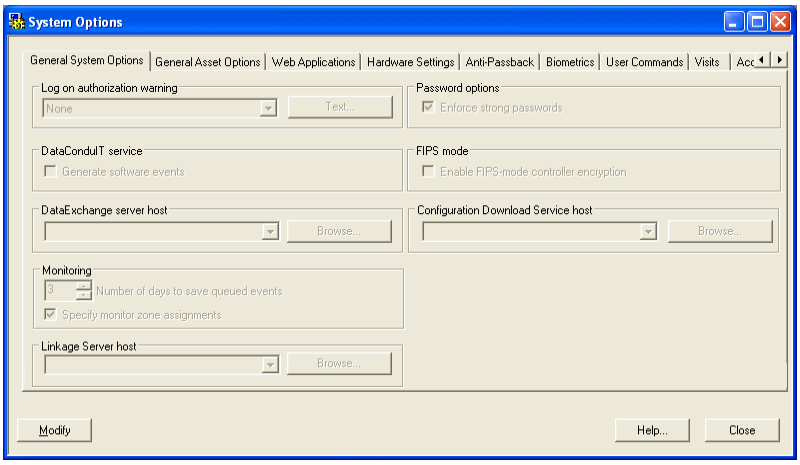
General System Options Form

The General System Options form is used to:

- Indicate if and how users will be warned about unauthorized system access.
- Configure monitoring options.
- Specify the host computer for the Linkage Server, which directs automatic e-mail/paging messages in response to specific alarms.
- Specify whether the DataConduIT service will generate software events.
- Specify the system's current threat level.

IMPORTANT: It is advisable to determine and configure General System Options prior to entering any data into your system.

Note: This form displays in both segmented and unsegmented systems.



Log on authorization warning

Configures the text for the authorization warning that is displayed upon login to the application. The text will be displayed in an Authorization Notification window. Choices include:

- **None**: no authorization warning will be displayed upon login to the application. This is the default selection.
- **Standard**: the default authorization warning will be displayed upon login to the application. The text of the default warning is as follows: "Warning: This computer program is a private application, restricted to use by only those who have authorized user accounts. Unauthorized use of this application or any portion thereof constitutes a violation of the law, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible. Are you authorized to use this application?"
- **Custom**: activates the [Text] push button, which enables you to customize the authorization warning.

Text

This button is activated only when **Custom** is selected in the Display authorization Warning drop-down list. Click this button to open the Custom Authorization Text window, in which you can specify the authorization warning text and its display characteristics.

Number of days to save queued events

The system can be configured to queue events while no one is logged into a particular monitoring station. This is done by selecting the **Queue Events When Logged Out** check box on the Monitor Stations form of the Monitor Zones folder, when creating a monitoring assignment for the monitoring station.

Over time, if no one logs into the monitoring station, there may be many queued events. The **Number of Days to Save Queued Events** field provides a way to purge the database so that the events don't become too numerous.

Once a day (between 3 a.m. and 4 a.m.), the Communication Server removes from the database any queued events that are older than the number of days specified by this field. You can select a value in the range of 1 to 365 days. The default is 3.

Specify monitor zone assignments

If selected, you are able to choose which monitor zone to add a new controller to. By default this option is selected and when the controller is added to the system it is added to all the monitor zones. If selected, once you add a new controller a dialog window opens and allows you to select the monitor zone(s) to add the controller to.

Linkage server host

You can configure the system to automatically send e-mail and paging messages when a given alarm occurs. The *Linkage Server* performs the alarm to message linkages. This section configures the host computer that the Linkage Server runs on. Each installation can have only one Linkage Server, which can be configured to run either as an application or as a Windows service.

The Linkage server needs to be configured for use for destination assurance, e-mail, paging, guard touring, badge deactivate status, Global I/O, DataConduIT message queues, and Scheduler.

Workstation

Specify the computer that will contain the Linkage Server. Each installation can have only one Linkage Server; the server can be started on the specified computer only. Type the computer name or use the [Browse] button to select it. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a window from which you can select the name of a host server. Click [OK] to insert the selected name into the **Host** field.

Generate software events

If selected, the DataConduIT service will generate software events.

DataExchange server host

This section is used to configure the host computer that the DataExchange server runs on. Each installation can have only one DataExchange server, which can be configured to run either as an application or as a Windows service.

Workstation

Specify the computer that will contain the DataExchange server host. Each installation can have only one DataExchange server; the server can be started on the specified computer only. Type the computer name or use the [Browse] button to select it. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a window from which you can select the name of a host server. Click [OK] to insert the selected name into the **Host** field.

Enforce strong passwords

Select this check box if you want to enforce strong passwords. Note the following:

- Strong passwords cannot be blank.
- Strong passwords cannot be the same as the user name.
- Strong passwords cannot be certain keywords.
- Certain Oracle database account user name and password pairs are not allowed.
- All user password's are checked when a user logs into an application. If the user's password does not meet the above standards and the **Enforce strong passwords** check box is selected, the user will be required to change their password before logging in. If the user's password does not meet the above standards and the **Enforce strong passwords** check box is not selected, the user will receive a message that their password does not meet the above standards but will be allowed to continue.

KnoWho server

Contains the [Browse] button and the **Host** and **Port** fields. This section is used to configure the host computer that the KnoWho server runs on.

Host

Select a host server form the drop-down list. You can either type the name in the field, select a host from the drop-down list, or use the [Browse] button to view a list of available workstations.

You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a window from which you can select the name of a host server. Click [OK] to insert the selected name into the **Host** field.

Port

Specifies the port that is on the serial expansion unit or the back of the host server.

Enable FIPS-mode controller encryption

Determines whether the windows for configuring controller encryption will be visible. An administrator may choose to enable this option so the OnGuard user interface does not display things to users that don't apply to them. If this option is selected, the windows for configuring controller encryption that are normally in the following locations will not be visible:

- (Non-segmented systems only) System Options folder
- (Segmented systems only) Segments folder
- Encryption form in the Access Panels folder along with the Fire Panels, Intercom Devices, Personal Safety Devices, Receivers, Intrusion Panels, and POS Devices folders.

This setting is separate from the FIPS mode settings that are configured on the individual Communication Server(s) using the FIPS Mode Configuration Utility. This setting has no impact on whether FIPS mode is used; it only affects how System Administration works and what windows are displayed. To use FIPS mode, you must enable FIPS mode on the Communication Server(s) by running the FIPS Mode Configuration Utility.

After this check box has been selected, all encryption keys for controller encryption will be cleared out of the database.

Configuration Download Service host

The configuration download service host is used to send updates down to the controllers when access level assignment changes are made using the browser-based Area Access Manager application. Only one instance of this service can exist in a system.

To configure where this service runs, use the browse button to select a workstation for the Configuration Download Service host.

Modify

Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help

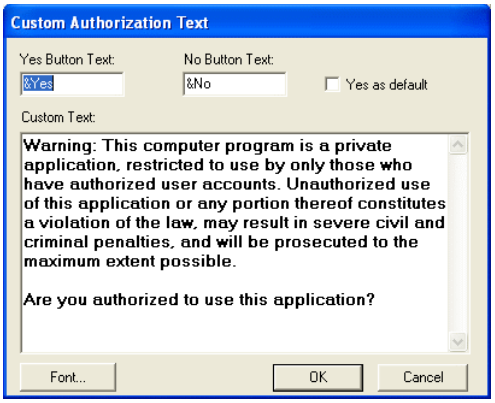
Displays online help information for this form

Close

Closes the System Options folder

Custom Authorization Text Window

This window is displayed by selecting “Custom” in the Log on authorization warning drop-down list and clicking [Text] on the General System Options form in the System Options folder.



Yes Button Text

Specifies the label that will be displayed on the [Yes] button in the Authorization Notification window. For example, OK/Cancel may be more appropriate choices for your notification than Yes/No.

You can underline one of the letters of the label, indicating that the letter can be used in combination with <Alt> as an accelerator key. To underline a letter for use as an accelerator key, place a “&” character immediately before it. For example, to specify the label “Valid” with the “a” underlined, type “V&alid”. <Alt>+<a> will be the accelerator.

No Button Text

Specifies the label that will be displayed on the [No] button in the Authorization Notification window. You can underline a letter for use as an accelerator key. For more information, refer to “Yes Button Text” definition in this table.

Yes as default

If this check box is selected, the [Yes] button will be the default button. If this check box is not selected, the [No] button will be the default button.

Custom Text

It is here that you type the actual text to be displayed in the Authorization Notification window.

Font

Opens a Font window, in which you can specify the display characteristics of the Authorization Notification window text. You can select the following from the options available on your computer:

- Font
- Font style (regular, bold, italic, etc.)
- Size (point size of the text)
- Script - lists language scripts available for the selected font
- Effects - (strikeout, underline, and color of text)

Sample displays sample text with the selected attributes applied.

OK

Saves your changes and closes the Custom Authorization Text window.

Cancel

Closes the Custom Authorization Text window without saving your changes.

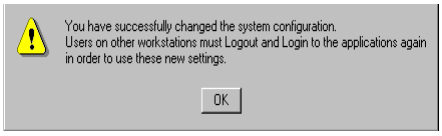
General System Options Form Procedures

Use the following procedures on this form.

Configure the Authorization Warning

1. On the General System Options form, click [Modify].
2. In the **Log on authorization warning** drop-down list, select the option that applies:
   - If you don't want users to be warned against unauthorized use when they log in, select **None**
   - If you wish to display the default warning, which is built into the system, select **Default**.
   - If you wish to display a customized warning, select **Custom**.

     To Customize the Warning:
     - Click [Text]. The Custom Authorization Text window will be opened.
     - Specify the label that will be displayed on the window's Yes and No buttons.
     - Specify whether or not the Yes button will be the default
     - Type the actual text of the warning as you wish it to appear in the window.
     - Choose the text's display characteristics.
     - Click [OK] to close the Custom Authorization Text window.
3. Click [OK] to save your General System Options settings.
4. If you have made changes using this form, the following message displays:

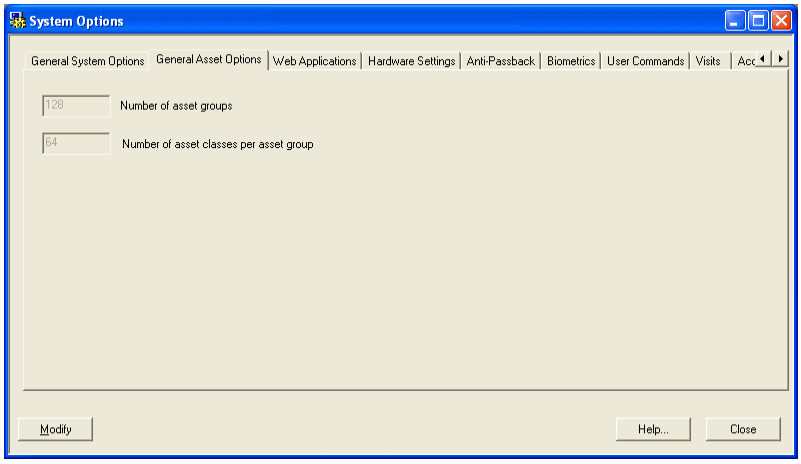


5. As the message indicates, any users that are currently accessing the system must log out then log in again.

General Asset Options Form

The General Asset Options Form is used to select the number of asset groups and number of asset classes per asset group for the system.

Note: This form displays in both segmented and unsegmented systems.



Number of asset groups

Set the number of asset groups. The default number of asset groups will be 128. The range that you are allowed to enter is from 1 to XXX.

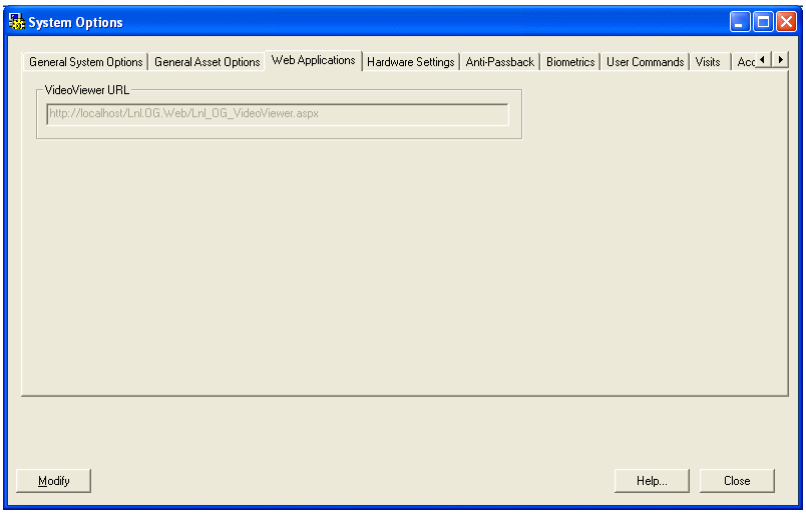
Number of asset classes per asset group

The default number of asset classes per asset group will be 64 but you can choose between a range of 1 to 64.

Web Applications Form

The Web Applications form is used to specify the VideoViewer URL to enable it to be launched from Alarm Monitoring.

Refer to the Installation Guide for information on installing and configuring the Web Application Server.



VideoViewer URL

Enter the web site address used to access VideoViewer. The default value is http://localhost/Lnl.OG.Web/Lnl_OG_VideoViewer.aspx. Depending on your network configuration, “localhost” should be replaced with the machine name, fully qualified machine name, or IP address of the web application server.

Modify

Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help

Displays online help information for this form.

Close

Closes the System Options folder.

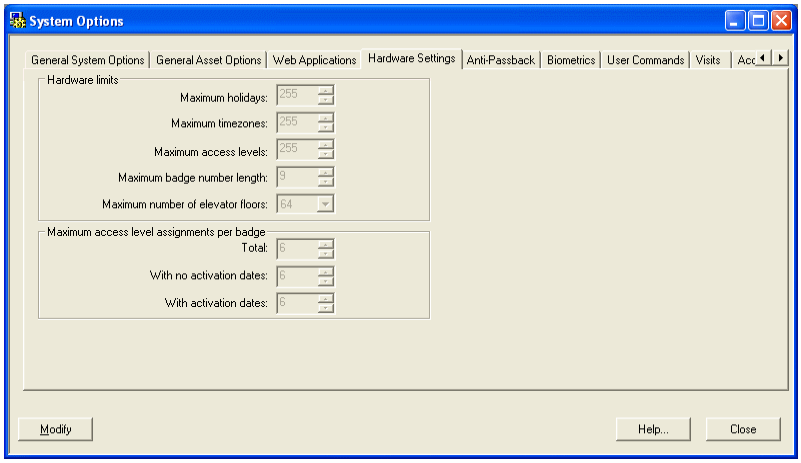
Hardware Settings Form

The Hardware Settings form is used to:

- Specify the maximum number of holidays, timezones, and access levels that can be defined in the system.
- Specify the maximum badge number length.
- Specify the maximum number of standard access levels, temporary access levels, and total access levels that can be assigned to an individual cardholder badge.

IMPORTANT: It is advisable to determine and configure Hardware Setting options prior to entering any data into your system.

Note: This form displays when segmentation is not enabled. When segmentation is enabled, these options are available in the Segments folder on the Hardware Settings sub-tab of the Segments form.



Maximum holidays

If you are using Lenel access panels, choose a value between 20 and 255 to specify the maximum number of holidays that can be defined in the system. The default is 255.

Maximum timezones

If you are using Lenel access panels, choose a value between 127 and 255 to specify the maximum number of timezones that can be defined in the system. The default is 255.

Maximum access levels

If you are using Lenel access panels, choose a value between 255 and 31,999 to specify the maximum number of access levels that can be defined in the system. The default is 255.

Maximum badge number length

Choose a maximum badge number length (number of digits). Lenel access panels support a maximum of an 18-digit badge number (maximum value 999,999,999,999,999,999).

If you create any temporary badges and import badge IDs to them, then the maximum badge number length must be increased to at least a value of 10.

Badge IDs require 4 to 8 bytes of memory when stored in access panels, depending on the number of digits in a badge.

- 9 digits or less require 4 bytes
- 10-12 digits require 5 bytes
- 13-14 digits require 6 bytes
- 15-16 digits require 7 bytes
- 17-18 digits require 8 bytes

Maximum number of elevator floors

Choose a maximum number of elevator floors to correspond with the floors in your building. The maximum number is 128.

Total

Specify the maximum number of access levels that can be assigned to a badge at one time. This includes both standard and temporary access levels. If you are using Lenel access panels, the maximum allowed is 128. If you reduce this number, you will be prompted that the application must proceed with a validation of each badge in the database to ensure that there are currently no badges that have more access level assignments than the value you are attempting to set. If there

exist badges that have too many assignments, a message box will display the badge ID that is in violation. If you wish to proceed, you must search up the badge in the Cardholders folder and reduce its access level assignments.

With no activation dates

Specify the maximum number of standard access levels that can be assigned to a badge at one time. *Standard access assignments* are regular assignments with no activate/deactivate date. In most cases, this will be set equal to the number entered in the **Total** field.

If you are using Lenel access panels, the maximum allowed is 128. This number cannot exceed the value in the **Total** field.

With activation dates

Specify the maximum number of temporary access level assignments that a badge can have. In most cases, this will be set equal to the number entered in the **Total** field. A *temporary access level* assignment is one that has been assigned an activate date, a deactivate date, or both.

If you are using Lenel access panels, the maximum allowed is 128. This number cannot exceed the value in the **Total** field.

Modify

Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help

Displays online help information for this form.

Close

Closes the System Options folder.

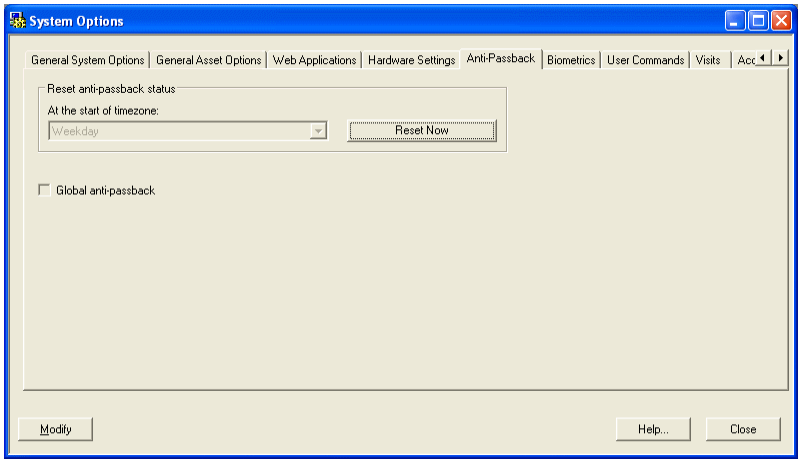
Anti-Passback Form

The Anti-Passback form is used to:

- Specify when to reset the anti-passback status for users associated with a given segment.
- Select whether the system will use global anti-passback.

IMPORTANT: It is advisable to determine and configure Anti-Passback options prior to entering any data into your system.

Note: This form displays when segmentation is not enabled. When segmentation is enabled, these options are available in the Segments folder on the Anti-Passback sub-tab of the Segments form.



At the start of timezone

Cards used in anti-passback readers will be made usable again at the beginning of the selected timezone. Choices include the names of all currently defined timezones.

Example: In situations where people may have left an area without swiping their cards through anti-passback readers (perhaps at the end of the work day) this insures that they will be allowed to reenter properly the next day.

Reset Now

This button is intended for use when a cardholder has committed an anti-passback violation and can't get into or out of a particular area.

If you click this button on a non-segmented system, a confirmation message that says "Are you sure you wish to reset global anti-passback status?" will be displayed. If you click [Yes], cards used in anti-passback readers will become usable again immediately.

If you click this button on a segmented system, a confirmation message that says "Are you sure you wish to reset global anti-passback status for segment *<segment name>*?" will be displayed. If you click the [Yes] button, cards used in anti-passback readers in the selected segment will become usable again immediately.

Global anti-passback

If selected, global anti-passback features can be used. When this check box is not selected the Areas folder only contains the Anti-Passback Areas form. When this check box is selected, the Areas folder contains the Anti-Passback Areas, Associated Safe Locations, Associated Inside Areas, and Muster Reporting forms.

Modify

Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help

Displays online help information for this form.

Close

Closes the System Options folder.

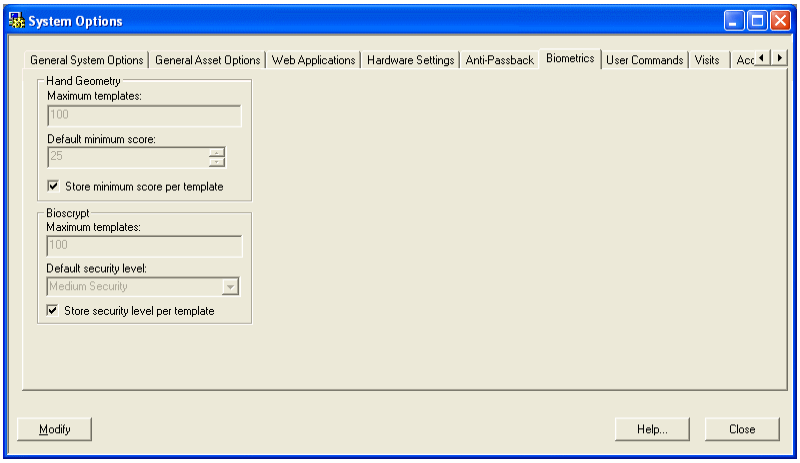
Biometrics Form

The Biometrics form is used to:

- Specify Hand Geometry biometric settings including maximum templates, default minimum score, and whether to store the minimum score per template.
- Specify Bioscrypt biometric settings including maximum templates, default minimum score, and whether to store the minimum score per template.

IMPORTANT: It is advisable to determine and configure biometric options prior to entering any data into your system.

Note: This form displays when segmentation is not enabled. When segmentation is enabled, these options are available in the Segments folder on the Biometrics sub-tab of the Segments form.



Hand Geometry

Maximum templates

Enter the maximum number of templates that can be downloaded to the controller.

The maximum number of templates is limited by the amount of free space on the controller. Each hand print template occupies 20 bytes. A total of 22 bytes are required per template if individual scores are stored with the template. Additional memory is required to enable HandKey support. For more information, refer to LNL-2000 (Options Sub-tab) on page 589.

Default minimum score

Choose the minimum score required to accept a template match between the access control reader and the template in the database. The lower the specified score, the closer the match must be during the verification process. Scores range from 1-255, with the default score being 25.

Store minimum score per template

Select this check box if you want minimum acceptance scores to be stored on a per template basis. If this check box is selected and the given template has a minimum acceptance score, the default will be overridden. If not selected, the default will be used.

Bioscrypt

Maximum templates

Enter the maximum number of templates that can be downloaded to the LNL-2000 controller. Only LNL-2000 controllers support Bioscrypt (V-Flex, V-Station or MV-1200) biometrics.

The maximum number of templates is limited by the amount of free space on the controller. Each fingerprint template occupies 362 bytes. Additional bytes are not required if individual scores are stored with the template because of the way the system rounds to the nearest even number. Additional memory is required to enable Bioscrypt support. For more information, refer to LNL-2000 (Options Sub-tab) on page 589.

Default security level

Select the default security level from the drop-down list.

Store security level per template

Select this check box if you want the default security level to be stored on a per template basis. If this check box is selected and the given template has a default security level, the default will be overridden. If not selected, the default will be used.

Modify

Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help

Displays online help information for this form.

Close

Closes the System Options folder.

Biometrics Form Procedures

Use the following procedures on this form.

Configure Biometrics

Complete this procedure to configure the maximum number of templates that can be downloaded to the access panel, as well as the minimum score necessary for template verification.

Note: The default number of templates that can be downloaded to the access panel is zero. Therefore, you must change the default value. If you do not change the default value, data will not be sent to the access panel and the controller capacity status will not display in Alarm Monitoring.

1. From the ***Administration*** menu, select ***System Options***, or click the System Options toolbar button.
2. Click the Biometrics tab.
3. Click [Modify].
4. If you are working with HandKey:
   a. Enter the maximum number of templates to be downloaded to the controller.

b. Enter the default minimum score required to accept a template match between the template read at the reader and the template stored in the database.

Note: The lower the HandKey score, the closer the match must be during the verification process.

c. Select the **Store minimum score per template** check box if you want minimum acceptance scores stored on a per template basis. If this check box is selected and the given template has a minimum acceptance score, the default will be overridden. If not selected, the default will be used. You assign minimum acceptance scores to templates in Multimedia Capture.

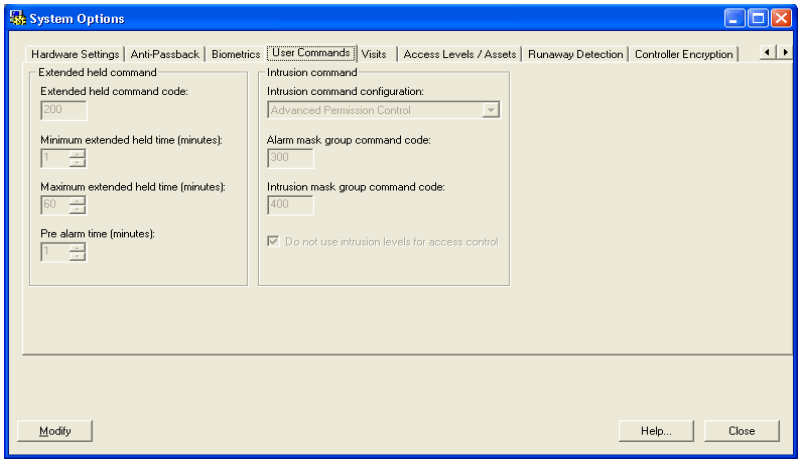
5. If you are working with Bioscrypt:
   a. Enter the maximum number of templates to be downloaded to the controller.
   b. Select the default security level which identifies the level of accuracy acceptable for template verification. Refer to the following table for rejection and acceptance rates per security level.

Security Level	False Rejection Rate	False Acceptance Rate
Very Low Security	1/10,000	1/100
Low Security	1/5,000	1/200
Medium Security	1/1,000	1/1,000
High Security	1/200	1/5,000
Very High Security	1/100	1/20,000

   c. Select the **Store security level per template** check box if you want to store individual security levels per template. Individual security levels are configured in Multimedia Capture. Leave this check box deselected if you want to use default security levels for all Bioscrypt templates.
      - If this check box is selected and the individual security level is set to “No Security”, then every Bioscrypt template will be successfully verified at the reader.
      - If this check box is not selected, then individual security levels are disabled, even though the security levels are still active in Multimedia Capture.
6. Click [OK].

User Commands Form

Note: This form displays when segmentation is not enabled. When segmentation is enable these options are available in the Segments folder on the User Commands sub-tab of the Segments form.



Extended held command code

The held open time for some readers can be extended by a validated user at a command keypad. This field indicates the key sequence to use for the command. The command code key sequence must be between three and six digits. The default is 200.

Minimum extended held time (minutes)

Indicates the minimum number of minutes to extend the held open time to. The default is one.

Maximum extended held time (minutes)

Indicates the maximum number of minutes to extend the held open time to. The default is 60.

Pre alarm time (minutes)

Indicates the pre alarm time in minutes. This is the number of minutes before the held open time expires that a pre alarm will be generated. The default is one.

Intrusion command configuration

Changing this option requires a database download to all access panels configured to be online.

Select from the following intrusion command options:

- **Disabled** - The default setting disables use of the intrusion command code.
- **Global Permission Control Only** - Allows use of the Alarm mask group command code only. For more information please refer to Appendix J: Intrusion Command on page 1469.You should also refer to Mask Groups Form on page 778.
- **Advanced Permission Control** -Allows the use of both the Alarm mask group command code and the Intrusion mask group command code separately according with the advanced functionality used for Command Keypad Templates. For more information, refer to Chapter 34: Command Keypad Templates Folder on page 743. You should also refer to Appendix J: Intrusion Command on page 1469..

Alarm mask group command code

If the **Global Permission Control Only** or **Advanced Permission Control** options are selected from the Intrusion command configuration drop-down box then the Alarm mask group command code can be configured. The command code can be between 3 and 6 digits in length and can not match the command code that is used by the extended held command code or intrusion mask group command code. For more information please refer to Appendix J: Intrusion Command on page 1469.

Intrusion mask group command code

The **Intrusion mask group command code** is only available for configuration when the Advanced Permission Control option is selected from the Intrusion command configuration drop-down list. The 'Intrusion mask group command code' number can be between 3 and 6 digits in length and can not match the command codes that are used for the Extended held command code as well as for the Alarm mask group command code. For more information please refer to Appendix J: Intrusion Command on page 1469.

Do not use intrusion levels for access control

Select to disallow cardholders automatic access control rights. To gain access control rights the cardholder must hold non-intrusion authority access levels. When this field is selected, intrusion authority levels assigned to a badge only allow control over executions of intrusion commands at the command keypad.

Setting this option requires a database download to all access panels configured to be online.

Modify

Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help

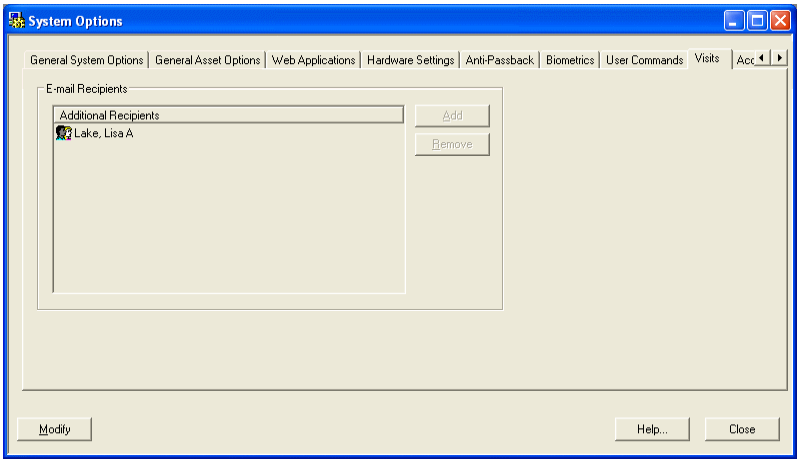
Displays online help for this topic.

Close

Closes the System Options folder.

Visits Form

Note: This form displays when segmentation is not enabled. When segmentation is enabled, these options are available in the Segments folder on the Visits sub-tab of the Segments form.



Additional Recipients listing window

The recipients listed are the default recipients who will be e-mailed if the **Default Recipients** check box is selected on the E-mail form in the Visits folder.

Add
In modify mode, click this button to open the Add recipient window, from where you can locate a recipient. For more information, refer to Chapter 5: Visits Folder on page 145.

Remove
In modify mode, click this button to remove the selected recipient from the Additional Recipients listing window.

Modify
Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help
Displays online help for this topic.

Close
Closes the System Options folder.

Visits Form Procedures

Use the following procedures on this form.

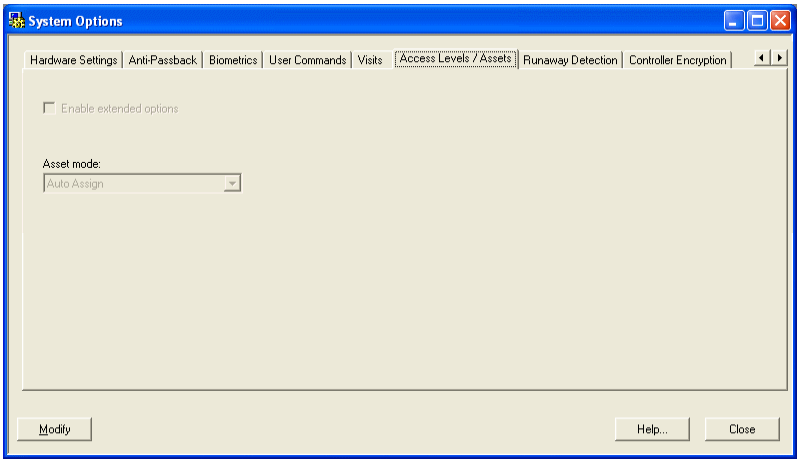
Configure Default E-mail Recipients

The recipients listed in the Additional Recipients listing window for a selected segment are the default recipients who will be e-mailed if the **Default Recipients** check box is selected on the E-mail form in the Visits folder. To configure the default e-mail recipients:

1. On a non-segmented system, select ***Administration*** > ***System Options***, then click the Visits tab. On a segmented system, select the ***Administration*** > ***Segments*** menu option, click the Segments tab, and then click the Visits sub-tab.
2. On a non-segmented system, just click [Modify]. On a segmented system, select a segment, then click [Modify].
3. Click [Add].
4. The Add recipient window opens. You may add a cardholder, visitor, directory account, or SMTP address.
   - If you select the Cardholder radio button and click [OK], the Select Host Wizard: Search form opens. For more information, refer to Select Host Wizard: Search Form on page 168.
   - If you select the Visitor radio button and click [OK], the Select Visitor Wizard: Search form opens. For more information, refer to Select Visitor Wizard: Search Form on page 171.
   - If you select the Directory account radio button and click [OK], the Select Account window opens.
   - If you select the SMTP address radio button, type the SMTP address, then click [OK]. An example of an SMTP address is “joesmith@company.com”.
5. Click [OK].

Access Levels/Assets Form

Note: This form displays when segmentation is not enabled. When segmentation is enabled, these options are available in the Segments folder on the Access Levels/Assets sub-tab of the Segments form.



Enable extended options

Select this check box to add escort functionality to access levels and enable the Access Levels/ Assets folder > Extended Options form. Extending options requires additional memory and a full access panel download. Users on other workstations must log out/on in order to use the new settings.

If a badge is using an escorted access level the badge should not also have the **Asset Format** check box selected when it is being configured. Doing so may result in errors when using the badge.

Asset mode

Choose the asset mode you wish to choose. Options include:

- **Tracking** - assets will be assigned to a specific individual (In Alarm Monitoring, an Asset Privilege Only message will always be generated.)
- **Auto Assign** - assets will be assigned based on Groups and Classes. A cardholder can belong to one Group. A Group contains Classes. Assets also contain Classes. When Auto Assign is selected, if the Assets Class matches the Group Class, then permission to have the asset is granted.

To disable asset operations, set the Assets field on the LNL-2000 or LNL-1000 form in the Access Panels folder to 0. It is advisable to determine and configure this option prior to entering any data into your system.

Modify

Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help

Displays online help for this topic.

Close

Closes the System Options folder.

Access Levels/Assets Form Procedures

Use the following procedures on this form.

Enable Extended Options for Access Levels

The following procedure applies to non-segmented systems only. For segmented systems, refer to the Segments folder on the Access Levels/Assets sub-tab of the Segments form.

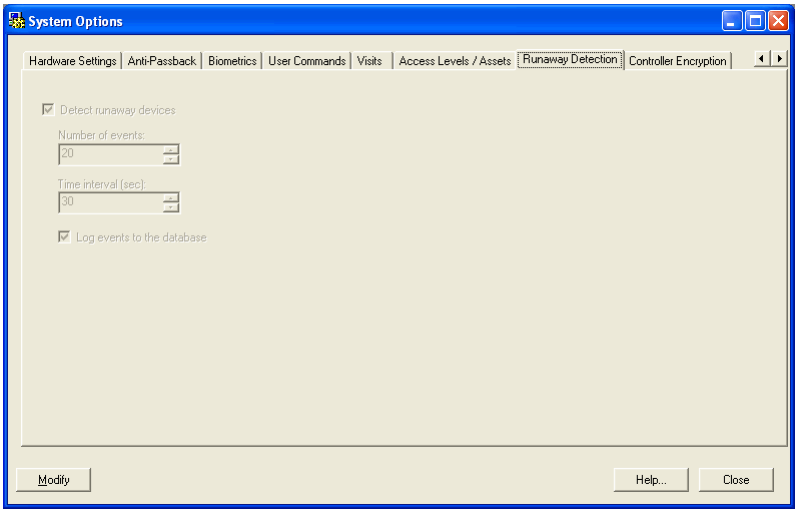
1. From the ***Administration*** menu, select ***System Options***, or click the System Options toolbar button.
2. Click the Access Levels/Assets tab.
3. Click [Modify].
4. Select the **Enable extended options** check box.

Note: To configure extend options for Access Levels (escort mode and activation times), refer to the Access Levels/Assets folder > Extended Options form. For more information, refer to Extended Options Form on page 729.

Runaway Detection Form

The Runaway Detection feature monitors the system for devices that have entered a “runaway” condition characterized by multiple alarms of the same type coming from a device during a user-defined time interval. Once this state has been identified it will be indicated in Alarm Monitoring by an alarm and by a change in state in the hardware tree. While in this state, the Communication Server stops sending the runaway events to Alarm Monitoring stations.

When the configured conditions for the runaway state are no longer true, a restored event will occur and the status will be returned to normal in the hardware tree.



Detect runaway devices

Select this check box to enable detection of runaway devices.

Number of events
Specify the number of events of the same type that must occur for a device to enter the runaway state.

Time interval (sec)
Specify the amount of time that the events must occur within for the device to enter the runaway state.

Log events to the database
Select this check box to continue logging the events to the database while the device is in a runaway state. Events will no longer be sent to Alarm Monitoring stations while the device is in a runaway state, but they can still be logged in the database.

Modify
Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help
Displays online help for this topic.

Close
Closes the System Options folder.

Controller Encryption Form

The Controller Encryption form is used to:

- Configure the system for encryption (automatic or manual)
- Enter master keys for encryption
- Export master keys to a text file
- Activate inactive keys (manual encryption only)

For more information regarding encryption, refer to the Encryption for Controllers User Guide.

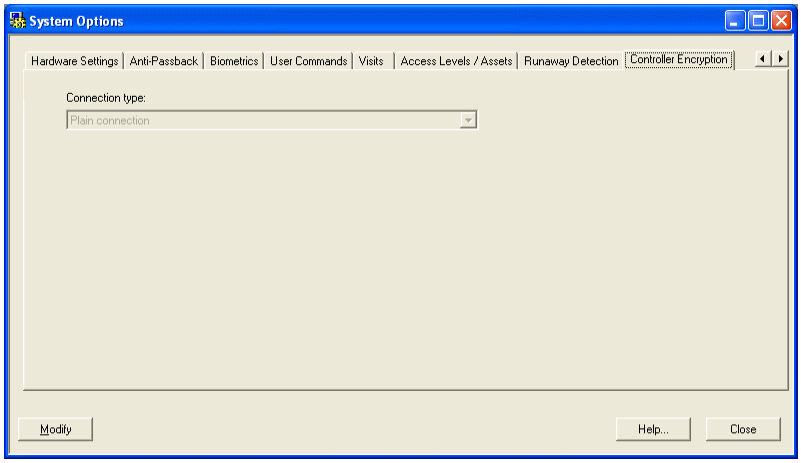
Note: This form displays when segmentation is not enabled. When segmentation is enabled, these options are available in the Segments folder, of the Segments form, on the Controller Encryption sub-tab.

To open the Controller Encryption form, select ***System Options*** from the ***Administration*** menu and click the Controller Encryption tab.

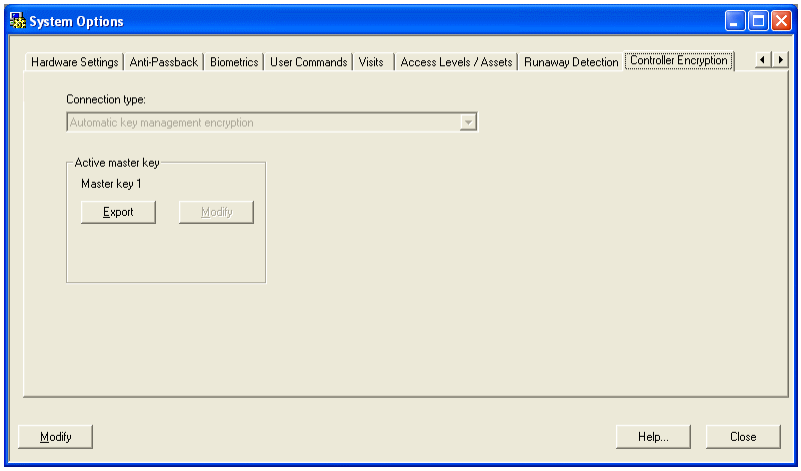
The Controller Encryption form is used to configure encryption for a system. This applies to Lenel controllers, Fire panels (ESPA, Notifier AM2020/NFS-640, Pyrotronics), Intercom Devices, Personal Safety Devices (Visonic Spider Alert), Receivers (Bosch 6500, SIA), Intrusion Panels (all except generic Intrusion), and POS Devices (TVC-2100 series). For more information, refer to the Access Panels Folder chapter.

The Controller Encryption form displays different fields depending on the connection type.

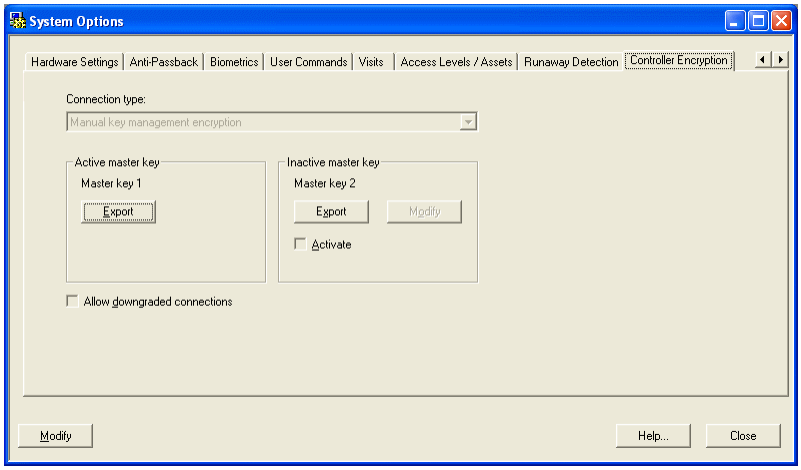
Plain Connection



Automatic Key Management Encryption



Manual Key Management Encryption



Connection type

The type of connection that exists between the controller and the host application. The default value is a plain connection.

Active master key

Displays the name of the active key, an export button and depending on the connection type, a modify button. If the connection type is automatic, the modify button displays. If the connection type is manual, the modify button does not display.

Active master key - Export

Exports the active master key to a text file. Depending on the status of your system, this may be master key one or two.

Active master key - Modify

Opens the Master Key Entry window where you can modify the active master key (one or two).

Note that you cannot modify the active master key using manual key management encryption; doing so would cause communication errors.

Inactive master key

Displays to the right of the Active master key section, regardless of which key is in/active. The inactive master key section includes the name of the inactive key, export and modify buttons, and the **Activate** check box. Displays only for manual key management systems.

Inactive master key - Export

Exports the inactive master key to a text file. Depending on the status of your system, this may be master key one or two. Displays only for manual key management systems.

Inactive master key - Modify

Opens the Master Key Entry window where you can modify the inactive master key. Depending on the status of your system, this may be master key one or two. Displays only for manual key management systems.

Activate

Select this check box when you want OnGuard to begin using this key. Displays only in the inactive master key section for manual key management systems. You should not activate a master key until both the controller and OnGuard have the same value for the inactive key.

If using an encrypted connection to one of the supported panels (Fire, Intercom, Personal Safety, Receiver, Intrusion or POS Devices) do not activate a master key until both the encrypted communication device and OnGuard have the same value for the inactive key

Allow downgraded connections

Select this check box if you want the host/controller connection to downgrade the connection if the encryption connection fails. Displays only for manual key management systems. (See Downgraded Connections, on page 413 for details.)

OK

Saves the changes made to the Controller Encryption form.

Cancel

Cancels the recent changes made to the Controller Encryption form.

Help

Displays online help for this topic.

Close

Closes the System Options Folder.

Downgraded Connections

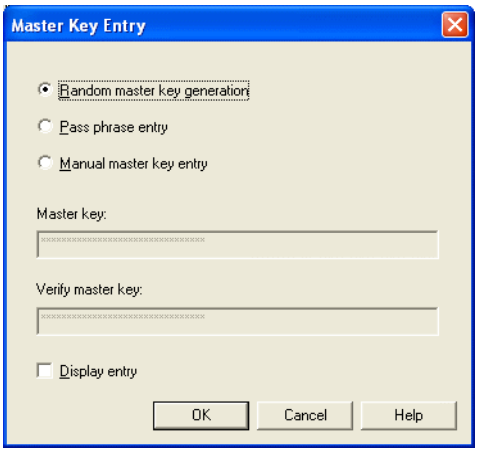
When the **Allow downgraded connections** check box is selected, the access control system attempts the following connections (in sequence):

1. An encrypted connection with the inactive master key
2. An encrypted connection with the factory default value for Master Key 1
3. An encrypted connection with the factory default value for Master Key 2
4. A plain connection (only attempted if the controller does not require an encrypted connection)

If encryption is enabled the following connections are attempted in sequence:

1. An encrypted connection with the inactive master key.
2. A plain connection.

Master Key Entry Window



Random master key generation

Randomly generates a 128-bit value master key and automatically populates the master key and verify master key text fields.

Pass phrase entry

Identifies the master key value as a pass phrase or sentence. When you select this radio button, you need to enter and verify the pass phrase in the corresponding text fields. The recommended minimum length for a pass phrase is 50 characters. The range of acceptable character length is between 1 and 255 characters. Spaces and symbols can be used and the pass phrase is case-sensitive.

Notice when this radio button is selected, the text fields on this form change to Pass phrase and Verify pass phrase.

Manual master key entry

Identifies the master key value as a 128-bit value in hexadecimal form. A 128-bit hexadecimal value is exactly 32 digits containing any of the following numbers or letters: 0 – 9, A – F. When you select this radio button, you need to enter and verify the master key in the corresponding text fields.

Master key/Pass phrase

The master key or pass phrase value. If you selected the random master key generation radio button, this field is automatically populated. If you selected the Pass phrase entry or Manual master key entry radio button, enter the master key/pass phrase.

Verify master key/Verify pass phrase

The master key or pass phrase value. Enter the master key/pass phrase field to verify that you correctly entered the master key/pass phrase value. You cannot copy/paste between this field and the master key/pass phrase field.

Display entry

Displays the characters in the master/pass phrase fields if this check box is selected.

OK

Accepts the changes and closes the Master Key Entry window.

Cancel

Closes the Master Key Entry window.

Help

Displays online help for this topic.

Controller Encryption Form Procedures

Use the following procedures on this form.

Configure Automatic Encryption and Set Keys

Note: The encryption modify/export permission is required to complete this procedure.

1. From the ***Administration*** menu, select ***System Options***, or click the System Options toolbar button.
2. Click the Controller Encryption tab. The Controller Encryption form opens.
3. Click [Modify].
4. If you are initially setting up automatic encryption:

Note: When encryption is being used with an encrypted communication device, the encryption key must be configured properly within the communication device first. The master key should then be configured on the Controller Encryption form For more information, refer to Controller Encryption Form on page 410.

   a. Select “Automatic key management encryption” from the **Connection type** drop-down list.
   b. Acknowledge any messages that display.
   c. Skip to step 5.

5. If you are updating the master key, click [Modify] (located in the active master key section of the form).
6. The Master Key Entry window opens. Select the **Manual master key entry**, **Pass phrase entry**, or **Random master key generation** radio button.
   - If you selected the **Manual master key entry** or **Pass phrase entry** radio button:

i. Select the **Display entry** check box if you want to see the characters you are typing.
ii. Enter and verify the master key/phrase. If the key is stored in a text file, you can copy/paste the key into these fields.
iii. Click [OK].
iv. Acknowledge any messages that display.

- If you selected the **Random master key generation** radio button:
  i. Select the **Display entry** check box if you want to see the master key values.
  ii. Click [OK].

7. On the Controller Encryption form, click [OK].
8. Acknowledge any messages that display.

Configure Manual Encryption and Set Keys

When you initially configure manual encryption, you should modify both master keys to prevent a key with a factory default value from being used (security risk).

If encryption is being used for Lenel access control panels (LNL-3300, 2220, 2000, 1000 and 500) then when you manually update a master key, you modify the inactive key and use the Lenel Controller Encryption Configuration Utility to load the new key into the controller. Once both the controller and OnGuard have the same value for the inactive key, you can activate the new key. For more information, refer to the Encryption for Controllers User Guide or the Lenel Controller Encryption Configuration Utility.

Notes: When encryption is being used with an encrypted communication device, the encryption key must be configured properly within the communication device first. Then the master key should be updated on the Controller Encryption form. Once the communication device and OnGuard have the same value for the inactive key, you can activate the new key.

The encryption modify/export permission is required to complete this procedure.

1. From the ***Administration*** menu, select ***System Options***, or click the System Options toolbar button.
2. Click the Controller Encryption tab. The Controller Encryption form opens.
3. Click [Modify].
4. If you are updating a key, skip to step 5. If you are initially setting up manual encryption, complete the following:
   a. Select “Manual key management encryption” from the **Connection type** drop-down list.
   b. Acknowledge any messages that display.
   c. Skip to step 6.
5. If you are updating a key, click [Modify] (located in the inactive master key section of the form).
6. The Master Key Entry window opens. Select the **Manual master key entry**, **Pass phrase entry**, or **Random master key generation** radio button.
   - If you selected the **Manual master key entry** or **Pass phrase entry** radio button:
     i. Select the **Display entry** check box if you want to see the characters you are typing.
     ii. Enter and verify the master key/phrase. If the key is stored in a text file, you can copy/paste the key into these fields.
     iii. Click [OK].
     iv. Acknowledge any messages that display.

- If you selected the **Random master key generation** radio button:
  i. Select the **Display entry** check box if you want to see the master key values.
  ii. Click [OK].

7. On the Controller Encryption form, click [OK].
8. Acknowledge any messages that display.
9. If manual encryption is enabled for the first time, it is recommended that you update both master keys by repeating this procedure.

Modify Master Keys

If you want to automatically update/change keys, refer to Configure Automatic Encryption and Set Keys on page 414.

If you want to manually update/change keys, refer to Configure Manual Encryption and Set Keys on page 415.

Export Master Keys

This procedure applies to manual and automatic key management encryption systems. To export master keys:

1. From the ***Administration*** menu, select ***System Options***, or click the System Options toolbar button.
2. Click the Controller Encryption tab. The Controller Encryption form opens.
3. Click [Export].
4. The Save As dialog opens. Enter the file name and click [Save].
5. Acknowledge any messages that display.

Activate Master Keys

The modify/export permission is required to complete this procedure.

1. From the ***Administration*** menu, select ***System Options***, or click the System Options toolbar button.
2. Click the Controller Encryption tab. The Controller Encryption form opens.
3. Click [Modify].
4. Select the **Activate** check box.
5. Select the **Allow downgraded connections** check box if you want the host to controller connection to downgrade to a plain connection when the encryption connection fails.
6. Click [OK].
7. Acknowledge any messages that display.

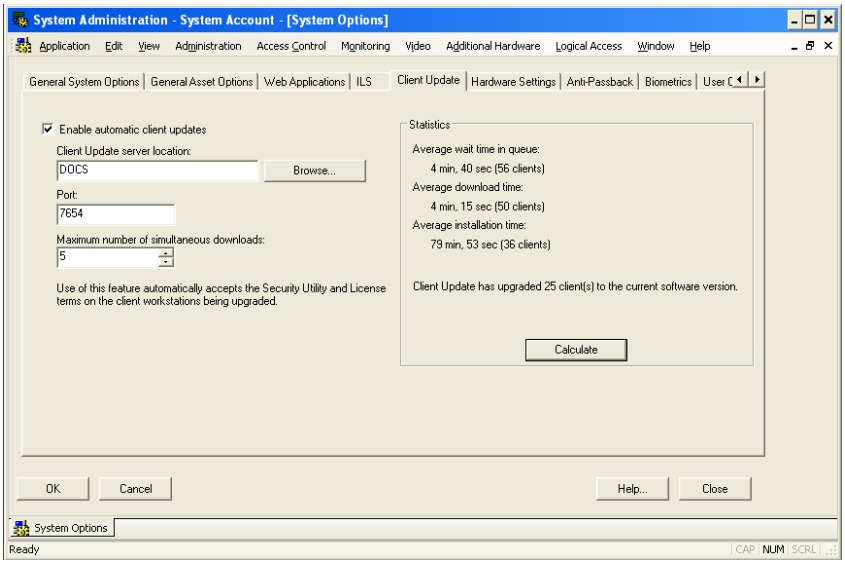
Client Update Form

The Client Update Server allows the OnGuard server workstation to automatically update client workstations. When a client workstation opens an OnGuard application, the application detects that the software version does not match the database. The application then allows the user to either cancel the login or update the client software. This functionality only exists for applications that are part of the OnGuard installation suite.

Two services enable this functionality, one installed on the server workstation (LS Client Update Server Service) and another installed on each client workstation (LS Client Update Service). These services are only used to update client workstations. Server workstations must still be updated manually. The server service is disabled by default.

Note: After enabling the automatic client updates feature, all Security Utility system modifications and license terms are accepted automatically on the client workstation being updated.

For more Automatic Client Update information, refer to Remote Installation of OnGuard in the Advanced Installation Topics guide.



Enable automatic client updates

Select this check box to enable the Client Update function for the entire system (or region for an Enterprise system).

Client Update server location

Click [Modify] and then browse to identify the server that hosts the update.

Port

This field allows you to configure the port used when downloading the update. By default, the port is 7654.

Maximum number of simultaneous downloads

Use this field to specify the maximum number workstations that can download from the server at the same time. The default is 5.

Statistics

This form area shows statistics for the Client Update function. Click [Calculate] to generate the following statistics:

- **Average wait time in queue:** The average time duration the client workstations have waited in the queue before the installation package download begins. Also identifies the number of client wait times used in this calculation.
- **Average download time:** The average time duration required to download the installation package. Also identifies the number of package downloads used in this calculation.

- **Average installation time:** The average time duration required to complete the Client Update installation. Also identifies the number of installations used in this calculation.

The form area also identifies the number of clients upgraded to the current software version. The number of clients shown might not be the same for each statistic. This occurs for several reasons, such as non-queued clients, incomplete downloads, incomplete installations, and so on. Also, the three Average statistics are based on the entire history of client updates which could span multiple software versions and hot fixes, but the Current Software Version client count is based on the current software release or hot fix only. Archived transactions are not included in these statistics.

For Enterprise systems, these statistics are specific to each server. For example, statistics on a master server apply to the master and its clients, but not the regions.

You can also run a detailed client update report. For more information, refer to Running a Client Update Report on page 419.

OK

Accepts the changes and closes the Client Update entry window.

Cancel

Closes the Client Update entry window.

Client Update Form Procedures

Use the following procedures on this form.

Enable and Configure Automatic Client Updates

Note: Only perform these configuration steps once for the entire system.

1. From the ***Administration*** menu, select ***System Options***, or click the System Options toolbar button.
2. Click the Client Update tab. The Client Update form opens.
3. Click [Modify].
4. Select the **Enable automatic client updates** check box.
5. Click [Browse], and then identify the location of the Client Update Server.
6. If the default port 7654 is acceptable, then leave the **Port** field unchanged. Otherwise, configure the port used when downloading the updates to the client workstations.
7. Configure the **Maximum number of simultaneous downloads** of client update files that the server will support at the same time. The default is 5.
8. Click [OK].
9. Start the LS Client Update Server Service on the workstation specified in step 5.

Client Update Troubleshooting

Issue

The client workstation does not ask users if they would like to perform an automatic upgrade after it determines that its version of OnGuard does not match the database.

Resolution

Confirm the following:

- Confirm that this is not a server installation. Automatic upgrades only work on client workstations.
- Automatic updates is turned on and configured. For more information, refer to Enable and Configure Automatic Client Updates on page 418.
- LS Client Update Server service is running and reachable on the configured host. On the server workstation, in Windows, go to ***Start*** > ***Control Panel*** > ***Administrative Tools*** > ***Component Services*** > ***Services (Local)*** and confirm that the LS Client Update Server service's status is Started.

  To confirm that you can reach the LS Client Update Server service, open a command prompt and ping the server using the `ping <configuredWorkstationName>` command.

  If the server service is not running and you get an error on startup, check the logs for details.
- The installed version of OnGuard is 6.5 or later. OnGuard 6.5 or later is required to provide automatic prompts to the user that an upgrade is available. To view the product version, open System Administration and select ***Help*** > ***About***.

  For client workstation versions of OnGuard earlier than 6.5, users can install an update without a disc if they receive and run the Client Update application.
- The installed version of OnGuard is newer than the database version. Run Database Setup on the server to update the database version.

Running a Client Update Report

To run a detailed report of the client update statistics:

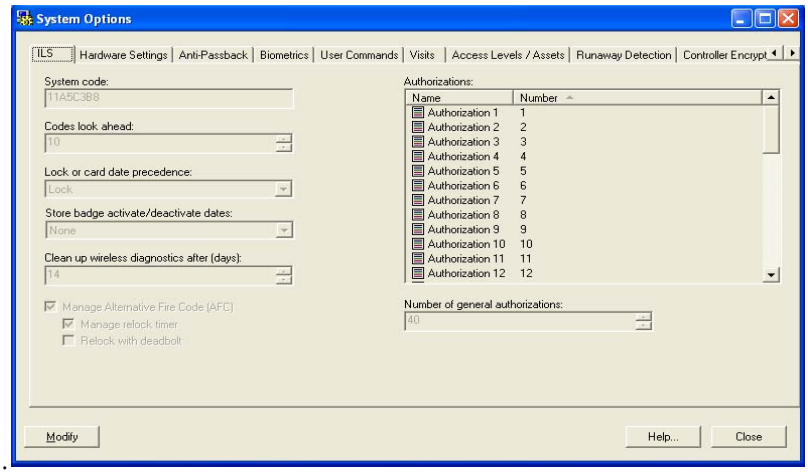
1. In System Administration, select ***Administration*** > ***Reports***.
2. Select the Date/Time Reports tab.
3. Select **User Transaction Log, By User ID**.
4. Configure the **Text Field Filter** as follows:
   - **Where:** Object
   - Equals
   - Client Update
5. Click [Preview].

ILS Form

Use the ILS form to configure data elements that affect the programming of all ILS controllers and locks in the system.

The default **System Code** should be modified by the system administrator and the system integrator prior to badge deployment and lock initialization. Failure to modify the **System Code** may cause corruption to wireless systems in close proximity (e.g. multi-tenant facilities). Retaining the default **System Code** will also lead to reduced facility security.

When you modify certain system settings, such as **System code** or **Store badge activate/deactivate dates**, this information must be downloaded to the XPP or Mobile Configurator in order to update or initialize the lock.



Note: In order to view this form, your system must have an ILS license.

System code

The system code is a unique identifier or name for the system.

Codes look ahead

This option applies to all ILS locks in the system. It tells the lock how many future codes it should allow for each user with access to that lock. Select from 5 - 99 with a default value of 10. Configuring this field to lower values provides greater system security.

Lock or card date precedence

This option specifies the date validation precedence at the lock, giving priority to the activate/deactivate date information on either the “Lock” or the “Card.” Initially the card data is downloaded to the lock, but the card data may eventually become out of sync with the lock data.

Store badge activate/deactivate dates

Specifies how the card activation/deactivation date information is stored on the badge. Choices include:

- None
- Date only
- Date and time

If you select “Date and time” ensure the **Use time** feature is enabled on the Cardholder Options > General Cardholder Options form.

Listing window

Lists the currently defined authorizations.

Number of general authorizations

Authorizations are used to limit access to areas without the need to update the locks. Authorizations allow you to customize accessibility to the locks as needed. There are 40 pre-defined authorizations that can be used. The number of general authorizations entered in this field controls the amount of authorizations that are available for assignment within the list when configuring badge types or cardholders.

Clean up wireless diagnostics after (days)

Allows all wireless diagnostics records stored longer than the number of days specified to be automatically purged. Configure from 1 - 30 days with a default value of 14 days.

Manage Alternative Fire Code (AFC)

The Alternative Fire Code (AFC) feature is used in jurisdictions where the local fire code specifies the locks cannot automatically relock behind a user exiting a room. Select this check box to allow this feature on a door-by-door basis. For more information, refer to the ILS Lock Operation User Guide.

Manage relock timer

Select to allow the door to relock after the door is unlocked after a specified amount of time. The time value is specified in the **Relock timer** field. For more information, refer to ILS Form on page 677.

The **Relock timer** field is only available form when **Manage relock timer** is selected during system configuration. Be sure to check with the local authorities to verify if this option is allowed within your jurisdiction.

Relock with deadbolt

Allows you to configure individual locks to lock automatically when the deadbolt is engaged.

Modify

Changes an ILS System Options entry.

Help

Displays online help information for this form.

Close

Closes the System Options folder.

ILS Form Procedures

To read how to configure an ILS locking system, refer to Appendix K: Lenel ILS (Integrated Locking Solutions) on page 1473..

CHAPTER 17

Cardholder Options Folder

The Cardholder Options folder contains forms with which you can:

- Modify general cardholder options
- Modify badge ID allocation options
- Modify visit options
- Modify logical access options
- Modify cardholder search results lists
- Modify visitor search results lists
- Modify visit search results lists
- Modify visit notification fields
- Modify person e-mail fields
- Link a cardholder field to an intercom panel type

The folder contains the following forms: the General Cardholder Options, Badge ID Allocation, Visits, Logical Access, Cardholder Search Results Lists, Visitor Search Results Lists, Visit Search Results Lists, Visit Notification Fields, Person E-mail Fields, and Automatic Lookup forms.

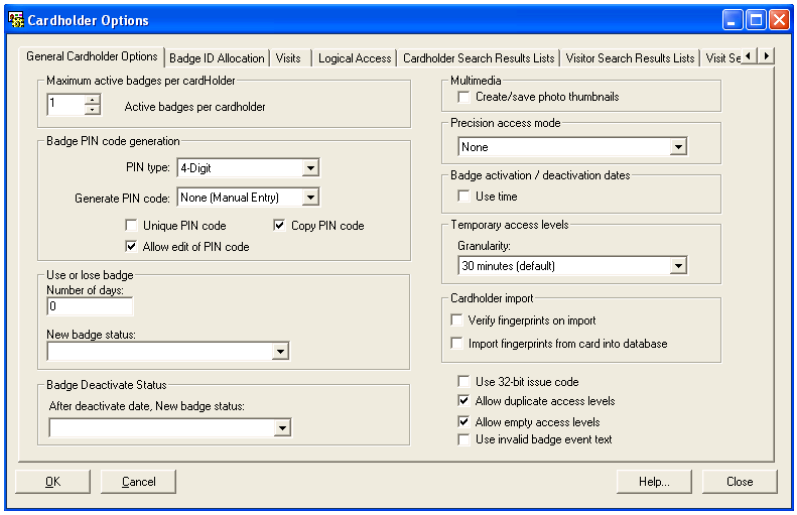
The Cardholder Options folder is displayed by selecting ***Cardholder Options*** from the ***Administration*** menu, or by selecting the Cardholder Options toolbar button.

Toolbar Shortcut

General Cardholder Options Form

The General Cardholder Options form is used to specify database guidelines for cardholder information, including maximum number of active badges per cardholder, PIN code, photo thumbnails, the status when a badge is not used for a period of time or has passed the deactivate date.

IMPORTANT: It is advisable to determine and configure General Cardholder Options prior to entering any data into your system.



Active badges per cardholder

Indicates the maximum number of active badges that are allowed for each cardholder. An active badge is one that was assigned the “Active” badge status using the Badge form in the Cardholders folder. The value must be at least 1, which is also the default. In most security systems, it is desirable to allow only one active badge per cardholder. However some installations require the ability to have more than one active badge per cardholder.

For example, if this value is set to “2”, you can define up to 2 active badges for an individual cardholder. If you attempt to add an additional active badge for a cardholder that already has two active badges, a Change Badge Status window opens, prompting you to change the badge status of one of the first two badges to something other than “Active.”

PIN type

Select the format for the PIN type. Choices include:

- 4-Digit - the PIN will contain 4 numbers
- 6-Digit - the PIN will contain 6 numbers
- 9-Digit - the PIN will contain 9 numbers

Changing the PIN type requires a full download.

System Administrators must log off/log on to the System Administration application before entering PIN numbers on the Cardholder folder-Badge form.

If you have a pin code configured for a controller that is 1-*n* digits long, but have a cardholder in the database that has a pin code longer than *n*, the pin code gets downloaded with the badge record, but gets truncated at *n* digits. For example, you have a 1-4 digit pin for the controller, but the badge record in the access control system’s database has ‘123456’ specified as the pin code. When this gets downloaded, it is truncated to ‘1234.’

Generate PIN code

Select the method by which a PIN code will be assigned upon creation of a new badge. Choices include:

- None (Manual Entry) - no PIN will be assigned. A PIN must be entered by the user who creates or changes the badge record.
- Random - the PIN will be assigned by the system. The number will be chosen randomly.

Unique PIN code

If selected, each cardholder badge record must have a unique PIN code. Otherwise, duplicate PIN codes will be allowed.

Copy PIN code

If selected, the **Copy PIN** check box in the Access Level and Pin Assignment form will be selected by default. Likewise, if it is not selected the **Copy PIN** check box will not be selected by default. For more information, refer to Add or Replace a Badge Record on page 114.

Allow edit of PIN code

If selected, a user having the appropriate privilege level will be able to change PIN values.

Number of days

For the use or lose badge feature, enter the number of consecutive days of badge inactivity after which badges will be assigned the badge status indicated in the **New badge status** field. A value of zero disables the use or lose badge feature.

New badge status

Select the badge status that will be assigned to badges when the **Number of days** value has been exceeded.

Choices in the drop-down list include default badge status values, and any badge status values that were added in the List Builder folder.

For information on the relationship between the use or lose badge settings (configured here) and use or lose badge type settings (configured in the Badge Types folder), refer to Use or Lose Badge on page 282.

After deactivate date, New badge status

Select the badge status that will be assigned to active badges when the deactivate date has passed. Choices in the drop-down list include default badge status values except for Active, and any badge status values that were added in the List Builder folder. If the field remains blank, the badge status will not be changed unless the badge deactivate status is set for the badge type.

For information on the relationship between the badge deactivate status settings (configured here) and badge deactivate status settings (configured in the Badge Types folder), refer to Badge Deactivate Status on page 282.

Create/save photo thumbnails

When a cardholder's photo is captured, by default it is saved in a high-resolution format in the database. If this check box is selected, the application immediately generates compressed, thumbnail versions for all existing cardholder photos. Any photos captured subsequently will be saved in both full-sized and thumbnail formats in the database.

The Cardholder View Options determine how photos are displayed. (To set Cardholder View Options, select ***Cardholders*** from the ***Administration*** menu, and then select ***View Options*** from the ***Cardholder*** menu.). If "Normal image" or "Normal image with chromakey" is selected in the **Cardholder photo lookup** drop-down, the uncompressed photo is displayed. If "Thumbnail" is selected in the **Cardholder photo lookup** drop-down, a smaller thumbnail version of the photo is displayed. Although the thumbnail photo has a lower resolution than the full-sized image, it displays faster–particularly when you have a slow network connection to the database. The "Thumbnail" option will not be available until this check box is selected and thumbnails have been created and saved.

If this check box was previously selected and you deselect it, the application immediately deletes all thumbnails currently in the database, leaving the full-sized versions alone. Any photos captured subsequently will be saved in the database in a full, uncompressed format only.

Because most organizations want to view the highest quality cardholder photos and don't really need/want to have optional draft versions, this check box is typically not selected. Selecting this check box requires more database space per image, since the thumbnail version of the image must be saved in addition to the full-size photo.

Precision access mode

Select the precision access mode for your installation. The option you choose applies to the entire system.

- None - Most people will choose this option, because the precision access features will typically be used only in very large, campus installations. Furthermore, the ability of Lenel hardware to manage up to 32,000 access levels and 32 level assignments per badge all but eliminates the need for precision access for any new installation. If you choose this option, the Precision Access forms in the Cardholders and Access Levels folders will not open.
- Inclusion - Choose this option to be able to select readers that an individual cardholder CAN access, and when (by specifying timezones)

Use time

Select this check box if you want to specify both date and time for badge activation/deactivation. When this check box is selected, the "Date and time" option will become available for selection in the **Store expiration date** and **Store activation date** drop-down lists on the Options sub-tab on the forms in the Access Panels folder. Note that only Lenel controllers can use time with badge activation and deactivation dates. For all other controllers, the time will always default to midnight.

Also, when this check box is selected, additional time controls will appear on the Badge form in the Cardholders folder. Modifications to this layout may be needed to properly handle these additional controls. Badge form layout modifications can be made in the FormsDesigner application. For more information, refer to the FormsDesigner User Guide.

Granularity

For date and time badge activation and deactivation purposes, the Linkage Server examines and updates temporary access levels several times a day (to determine if a badge needs to be added to or removed from a panel). By default, the temporary access levels are examined and updated every 30 minutes. If you choose, you can change this setting by selecting another value from this drop-down list.

It is important to consider that reducing the temporary access level granularity below the default setting (30 minutes) may impact system performance. (Because temporary access level processing will be performed more frequently, more resources may be consumed.)

Verify fingerprints on import

Select to enable fingerprint verification. If an OnGuard supported fingerprint scanning device is not available, this option must be disabled. For a list of supported scanner devices, refer to the Cardholder/Visitor Import table on page 104.

Import fingerprints from card into database

Select to enable the importing of fingerprint templates. By default, this option is not enabled since fingerprints are considered sensitive data, and some organizations may not want them copied off the card.

Use 32-bit issue code

Enabling this checkbox increases the size of the issue code from a single byte (8-bit) to 4 bytes (32-bit). When changing this setting the cardholder size changes, and so a database download is required. The cardholder record size will increase by 3 more bytes. This is a system wide setting so enabling it will affect your entire system. Currently the only hardware that can support a 32-bit issue code are the Lenel Intelligent System Controllers. If enabled, the first issue code used when generating badges can only have a maximum value of 99.

Allow duplicate access levels

This check box is selected by default. Disable this option to not allow duplicate access levels to be created.

Allow empty access levels

This check box is selected by default. If disabled, the user will be prompted when deleting an access panel or reader that results in an access level losing its reader assignments.

Use invalid badge event text

Select to enable/disable the invalid badge event text. The invalid badge event text is a system administrative user enabled feature that allows configured text to appear when an invalid badge event is received.

Modify

Used to change Cardholder Options. When clicked, settings can be changed on any form in the Cardholder Options folder.

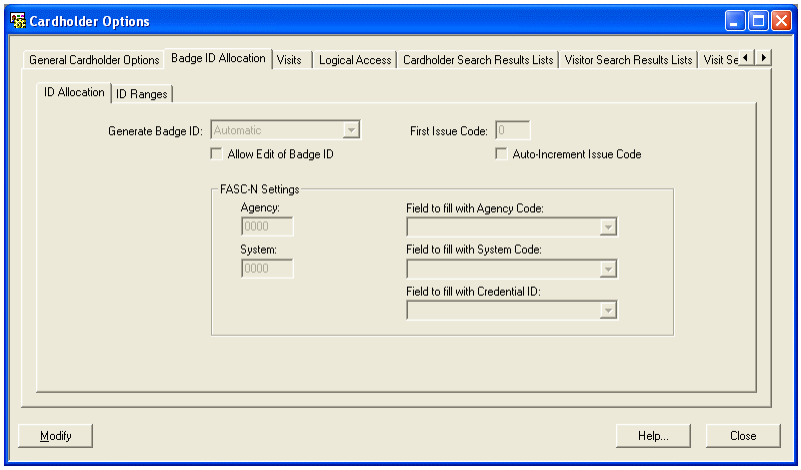
Help

Displays online assistance for this form.

Close

Closes the Cardholder Options folder

Badge ID Allocation Form - ID Allocation Sub-tab



Generate Badge ID

Select the method by which the **Badge ID** field will be automatically filled in when adding a new badge. Choices include:

- **Automatic** - the badge ID will be assigned by the system. Generally, each new badge ID will be the previous badge ID + 1. This applies even if you are creating a new badge for a cardholder who's already in the database, as would occur if the previous badge were lost or stolen.
- **FASC-N** - Refers to government issued badges. FASC-N is an acronym for Federal Agency Smart Credential Number. Selecting this causes the FASC-N Settings on this form to become enabled for you to use.
- **From 'Cardholder ID'** (or, if you have a custom cardholder layout, the custom field name will be indicated here) - uses the special cardholder fixed field. The name of this field may be different if you have a custom cardholder layout designed with FormsDesigner. Whatever you enter in this field will be used as the badge ID for that particular cardholder. With this setting the badge ID will always be the same for a cardholder - in this case, the issue code is used to distinguish between different badges for the same cardholder. Note that to use this setting the field upon which you are basing the badge ID must be all numeric data.
- **Internal Cardholder ID** - this option is similar to the "From 'Cardholder ID'" option except that this option uses a system-generated number as compared to a manually entered number. Functionally, the badge ID will always be the same for a cardholder. You must use a different issue code to distinguish between different badges for the same cardholder.
- **Manual Entry** - no badge ID will be automatically assigned. A badge ID must be entered by the user who creates the badge record.

Allow Edit of Badge ID

If selected, a user having the appropriate privilege level will be able to change badge ID values.

Leave this check box blank if you do not want a user to ever be able to edit the badge ID.

Note: If badge ID is generated From 'Cardholder ID' or Manual Entry, badge IDs can be edited BEFORE printing. Users with the Can edit ID/issue/type after printing permission can also edit badge IDs AFTER printing.

First Issue Code

If your installation uses issue codes on its badges, zero is used by default as the first issue code when you create a new badge. If your organization wants to use a different number, enter that number in this field.

Auto-Increment Issue Code

You can change (select or deselect) this value. However:

- This field is selected by default if you chose "From Cardholder ID" in the **Generate Badge ID** field on this form.
- This field is deselected by default if you chose "Automatic" in the **Generate Badge ID** field on this form. This is because each time you create a badge (even if it's for someone whose badge has been lost), a new badge ID will be assigned automatically. Therefore, it's considered to be a new card, and the issue code counter starts over again.

FASC-N Settings

This section of the form holds the settings used for FASC-N badges. To enable these you must select FASC-N from the **Generate Badge ID** drop-down.

Agency
A four digit code identifying the government agency issuing the credential. The agency code is just one part of 31 bits of information that will be encoded on the magnetic stripe of government smart cards. The agency code is also part of what becomes the OnGuard badge ID.

System
A four digit field identifying the system the card is enrolled in. Within an Agency the system must be a unique value. The system is just one part of 31 bits of information that will be encoded on the magnetic stripe of government smart cards. The system is also part of what becomes the OnGuard badge ID.

Field to fill with Agency Code
Specifies the field in the Cardholders folder > Badge form that will display the Agency Code. You can select from the default OnGuard fields or define a field using FormsDesigner.

Field to fill with System Code
Specifies the field in the Cardholders folder > Badge form that will display the System Code. You can select from the default OnGuard fields or define a field using FormsDesigner.

Field to fill with Credential ID
Specifies the field in the Cardholders folder > Badge form that will display the Credential ID. You can select from the default OnGuard fields or define a field using FormsDesigner.

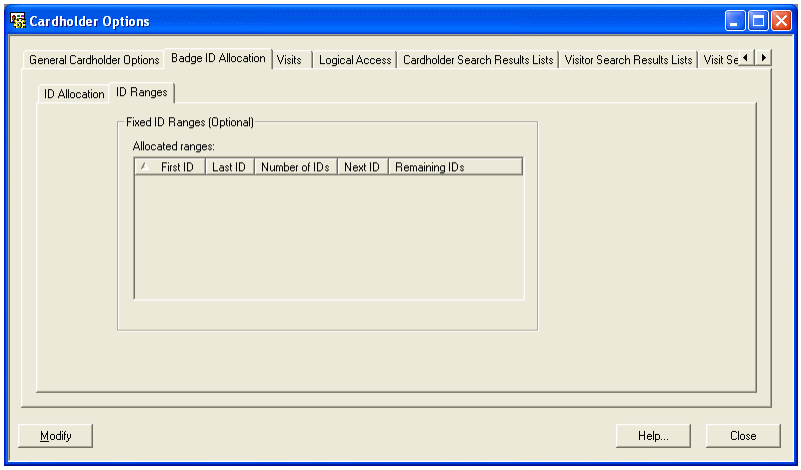
Modify
Used to change Cardholder Options. When clicked, options on any form in the Cardholder Options folder can be modified.

Help
Displays online assistance for this form.

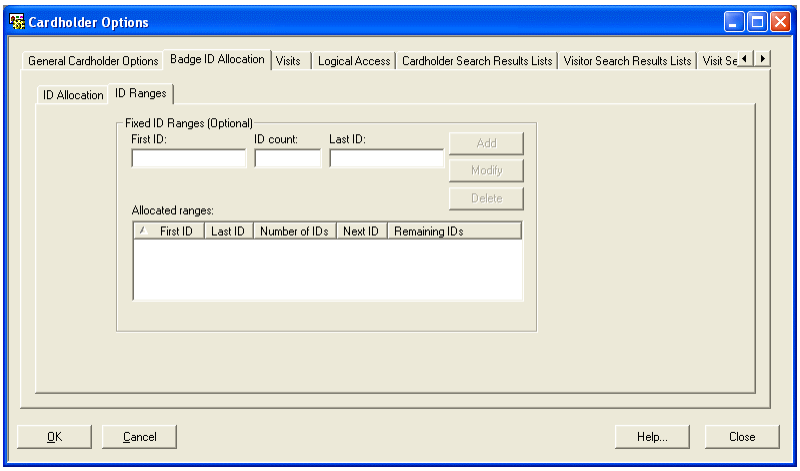
Close
Closes the Cardholder Options folder.

Badge ID Allocation Form - ID Ranges Sub-tab

Badge ID Allocation Form - ID Ranges Sub-tab (View Mode)



Badge ID Allocation Form - ID Ranges Sub-tab (Modify Mode)



Fixed ID Ranges (Optional)

In view mode, contains the **Allocated ranges** display field. In modify mode, contains the **First ID**, **ID count**, and **Last ID** fields. Also contains the [Add], [Modify], and [Delete] buttons as well as the **Allocated ranges** display field.

Allocated ranges listing window

Displays the first and last ID number that will be used, as well as the number of IDs, next ID, and remaining IDs.

First ID (displayed only in modify mode)

Type the first ID number to be used. If you enter the first ID and ID count, the **Last ID** will automatically be determined and filled in.

ID count (displayed only in modify mode)

Type the number of IDs you wish to use. If you enter the ID count and first ID, the last ID will automatically be determined and filled in.

Last ID (displayed only in modify mode)

This is the last number that will be allocated as an ID. As long as the **First ID** and **ID count** fields have numeric values entered, the **Last ID** field will automatically be determined and filled in.

Add (displayed only in modify mode)

This button is enabled only when valid data is entered in the **First ID**, **ID count**, and **Last ID** fields. Its function is to add the range specified in the **First ID**, **ID count**, and **Last ID** fields to the Allocated ranges listing window.

Modify (displayed only in modify mode)

This button is enabled only when an entry is selected in the Allocated ranges listing window. Its function is to modify the range that is selected in the Allocated ranges listing window when a new value is entered in the **First ID**, **ID count**, or **Last ID** fields.

Delete (displayed only in modify mode)

This button is enabled only when an entry is selected in the Allocated ranges listing window. Its function is to delete the range that is selected in the Allocated ranges listing window.

Modify

Used to change Cardholder Options. When clicked, options on any form in the Cardholder Options folder can be modified.

Help

Displays online assistance for this form.

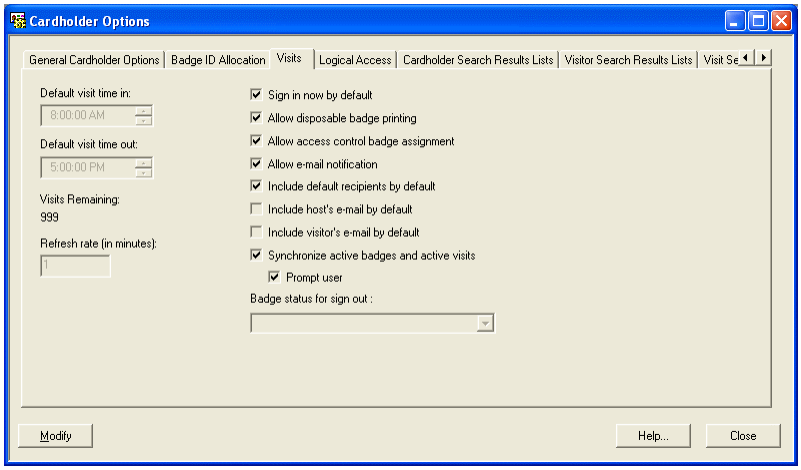
Close

Closes the Cardholder Options folder.

Visits Form

The Visits form is used to specify database guidelines for cardholder information, including default visit time in and out, the badge status set when a badge is signed out, and other visit options. This form is also used to specify options for the Front Desk if it is in use.

IMPORTANT: It is advisable to determine and configure Visit options prior to entering any data into your system.



Default visit time in

Select the time that visits begin by default. This time will become the default time that is displayed in the **Time in** field on the Visit form in the Visits folder and/or the Front Desk.

There are four sections in this field: hour, minute, second, and AM/PM. Click on the section of the time you would like to adjust, and then do one of the following to adjust it:

- Click the up arrow to increase a numerical value, or the down button to decrease a numerical value. For AM/PM, the arrow buttons toggle between the two settings.
- Type the numerical time value, typing a colon in between each value. For example, to enter the time 6:00:00 AM, type 6:00:00:AM.

Default visit time out

Select the time that visits end by default. This time will become the default time that is displayed in the **Time out** field on the Visit form in the Visits folder and/or the Front Desk.

There are four sections in this field: hour, minute, second, and AM/PM. Click on the section of the time you would like to adjust, and then do one of the following to adjust it:

- Click the up arrow to increase a numerical value, or the down button to decrease a numerical value. For AM/PM, the arrow buttons toggle between the two settings.
- Type the numerical time value, typing a colon in between each value. For example, to enter the time 6:00:00 AM, type 6:00:00:AM.

Visits Remaining

Indicates the number of visits that can be specified. This number is determined by subtracting one from the maximum number of visits specified in the OnGuard license each time a visit is scheduled.

Refresh rate (in minutes)

This refresh rate determines the default value for the **Refresh rate (in minutes)** field on the Status search form in the Visits folder and/or the Front Desk. The refresh rate is how often the database is queried to see if it has changed. This refresh rate only applies when searching based on a status (i.e., the “Scheduled, future”, “Scheduled, late”, “Active”, “Active, overstayed”, or “Finished” status) on the Status search form in the Visits folder.

Although this setting determines the default value, the refresh rate on the Status search form in the Visits folder can be changed by a user when a search is done.

Sign in now by default

If selected, the **Sign in now** check box will be selected by default when a visit is added, the visit will automatically be signed in, and the **Time in** field for the visit will be updated with the current time.

If not selected, the **Sign in now** check box will not be selected by default when a visit is added. The [Sign In] button will be available. When the [Sign In] button is clicked, the visit will be signed in, and the **Time in** field for the visit will be updated with the current time.

Allow disposable badge printing

If selected, the user can print a disposable badge by selecting a disposable badge type to be assigned and printed when adding a visit.

Allow access control badge assignment

Enables assigning an access control badge on visit sign in. If enabled, the user will be able to type in the badge ID of an existing visitor badge when signing in a visit. The badge must already exist in the system, and its badge type must be of the class “Visitor”.

Allow e-mail notification

If selected, e-mail notifications can be sent for visits. For this feature to work, an SMTP server must be configured in the Global Output Devices folder.

Include default recipients by default

If selected, the Default Recipients check box on the E-mail form in the Visits folder will be selected by default when a new visit is added. (If a visit is added based on a currently selected record, the setting for that record will be used instead of the default.). To configure the default recipients:

- On segmented systems, select ***Administration*** > ***Segments***, click the Segments tab, then click the Visits sub-tab. On the Visits sub-tab, you can add or remove recipients. These recipients will be collectively considered the “Default Recipients” on the E-mail form in the Visits folder.
- On nonsegmented systems, select ***Administration*** > ***System Options***, then click the Visits tab. On the Visits tab, you can view or modify the default recipients.

Include host's e-mail by default

If selected, the **Cardholder for this visit** check box on the E-mail form in the Visits folder will be selected by default when a new visit is added. (If a visit is added based on a currently selected record, the setting for that record will be used instead of the default.)

Include visitor's e-mail by default

If selected, the **Visitor for this visit** check box on the E-mail form in the Visits folder will be selected by default when a new visit is added. (If a visit is added based on a currently selected record, the setting for that record will be used instead of the default.)

Synchronize active badges and active visits

If selected, synchronizes the badge activation and deactivation date with the visit time in and visit time out. A visitor's badge is activated at the beginning of the day the visit is scheduled for and deactivated at the end of the day that the visit is scheduled for. For more information, refer to Synchronize Active Badges with Active Visits on page 445.

Prompt user

If the **Synchronize active badges and active visits** and **Prompt user** check boxes are selected, active badges will be synchronized with active visits, and you will be prompted before the synchronization occurs. The prompt gives you a clear understanding of what is being synchronized, and allows you to choose which badges will be synchronized if the visitor has multiple active badges.

If the **Synchronize active badges and active visits** is selected but the **Prompt user** check box is not selected, all active badges and active visits will be synchronized, and you will not be prompted when they are synchronized. If a visitor has multiple active badges, you will not be able to choose which active badges get synchronized; they will all get synchronized.

Badge status for sign out

Allows the user to choose the default badge status to change active badges to when the [Sign Out] button is pressed. Choices include all currently recognized Badge Statuses, which are defined on the Simple Lists form of the List Builder folder. Default choices that are defined include Lost or Returned.

Modify

Used to change Cardholder Options. When clicked, settings can be changed on any form in the Cardholder Options folder.

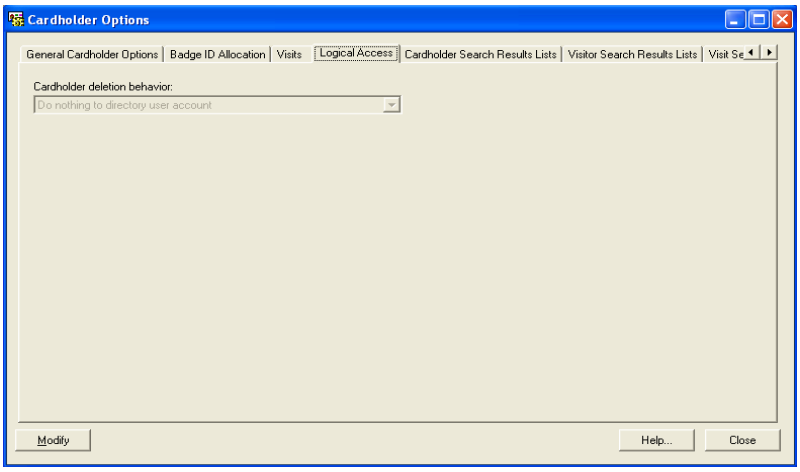
Help

Displays online help for this form.

Close

Closes the Cardholder Options folder.

Logical Access Form



Cardholder deletion behavior

Determines the action that will take place on the cardholder's linked logical user account when the cardholder is deleted.

Modify

Used to change Cardholder Options. When clicked, settings can be changed on any form in the Cardholder Options folder.

Help

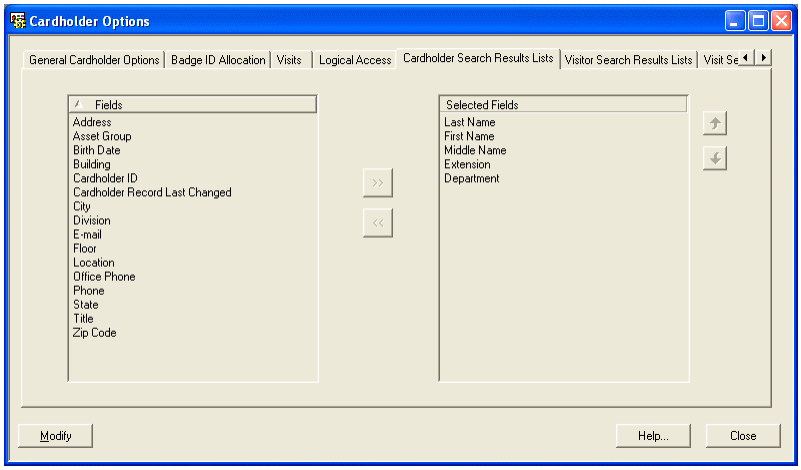
Displays online help for this form.

Close

Closes the Cardholder Options folder.

Cardholder Search Results Lists Form

The Cardholder Search Results List form is used to specify database guidelines for which information will be displayed when a cardholder is searched for and in what order this information will be displayed.



Fields

Displays the list of fields available to be displayed in the Cardholder search results.

Selected Fields

Displays the list of fields that will be displayed in the order listed (from top to bottom) in the Cardholder search results.

Enabled only in Modify Mode. When clicked, moves a field that is selected in the Selected Fields display to the Fields display, effectively removing it from the Cardholder search results.

When clicked, moves a field that is selected in the Fields display to the Selected Fields display, effectively including it in the Cardholder search results.

Moves a field selected in the Selected Fields display up one position in the Cardholder search results.

Moves a field selected in the Selected Fields display down one position in the Cardholder search results.

Modify

Used to change Cardholder Options. When clicked, settings can be changed on any form in the Cardholder Options folder. On the Cardholder Search Results Lists form, allows the user to change the contents and order in the Cardholder search results lists.

Help

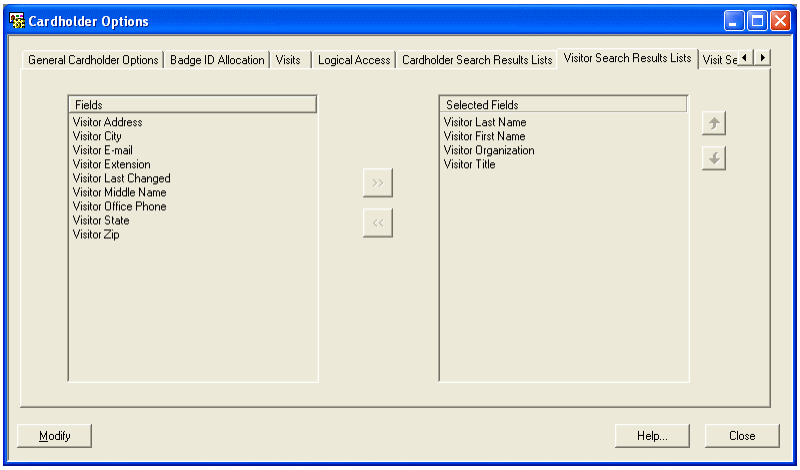
Displays online help for this form.

Close

Closes the Cardholder Options folder.

Visitor Search Results Lists Form

The Visitor Search Results Lists form allows the user to select the fields and display order to use for the visitors search results lists. User defined fields (UDFs) will be included.



Fields

Displays the list of fields available to be displayed in the Visitor search results.

Selected Fields

Displays the list of fields that will be displayed in the Visitor search results.

Enabled only in Modify Mode. When clicked, moves a field that is selected in the Selected Fields display to the Fields display, effectively removing it from the Visitor search results.

Enabled only in Modify Mode. When clicked, moves a field that is selected in the Fields display to the Selected fields display, effectively including it in the Visitor search results.

Moves a field selected in the Selected Fields display up one position in the Visitor search results.

Moves a field selected in the Selected Fields display down one position in the Visitor search results.

Modify

Used to change Cardholder Options. When clicked, settings can be changed on any form in the Cardholder Options folder. On the Visitor Search Results Lists form, allows the user to change the contents and order in the Visitor search results lists.

Help

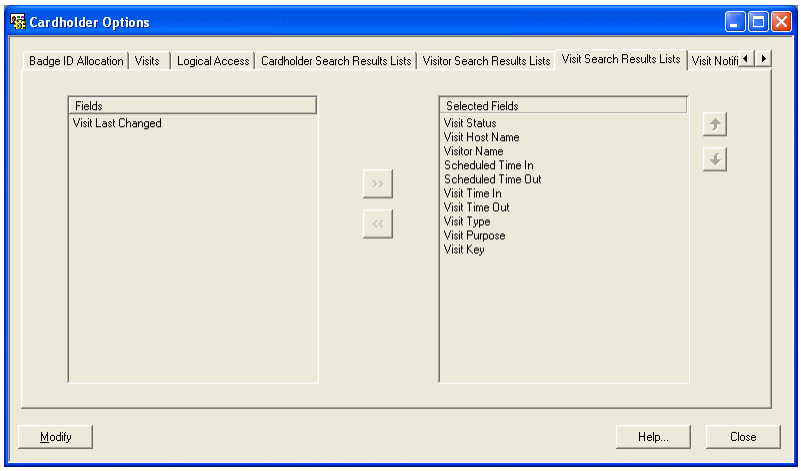
Displays online help for this form.

Close

Closes the Cardholder Options folder.

Visit Search Results Lists Form

The Visit Search Results Lists form allows you to select the fields and display order to use for the columns in the Visits listing window in the Visits folder.



Fields listing window

Displays the list of fields available to be displayed in the Visit search results.

Selected Fields listing window

Displays the list of fields that will be displayed in the Visit search results.

Enabled only in Modify Mode. When clicked, moves a field that is selected in the Selected Fields display to the Fields display, effectively removing it from the Visit search results.

Enabled only in Modify Mode. When clicked, moves a field that is selected in the Fields display to the Selected fields display, effectively including it in the Visit search results.

Moves a field selected in the Selected Fields display up one position in the Visit search results.

Moves a field selected in the Selected Fields display down one position in the Visit search results.

Modify

Used to change Cardholder Options. When clicked, settings can be changed on any form in the Cardholder Options folder. On the Visit Results Lists form, allows the user to change the contents and order in the Visit search results lists.

Help

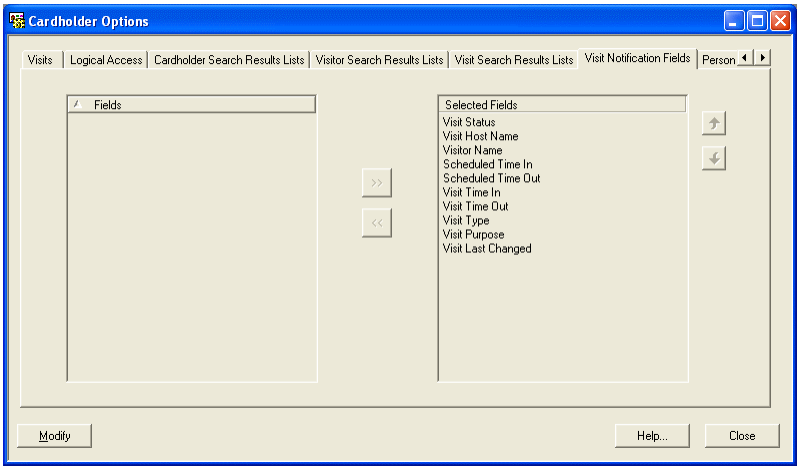
Displays online help for this form.

Close

Closes the Cardholder Options folder.

Visit Notification Fields Form

The Visit Notification Fields form allows you to select the fields and display order to use for the information that is included in visit notification e-mails.



Fields listing window

Displays the list of visit record fields that are available to be included in the body of e-mail notifications.

Selected Fields listing window

Displays the list of visit record fields that will be included in the body of e-mail notifications.

Enabled only in Modify Mode. When clicked, moves a field that is selected in the Selected Fields display to the Fields display, effectively removing it from the body of e-mail notifications.

Enabled only in Modify Mode. When clicked, moves a field that is selected in the Fields display to the Selected fields display, effectively including it in the body of e-mail notifications.

Moves a field selected in the Selected Fields display up one position in the e-mail notification's body.

Moves a field selected in the Selected Fields display down one position in the e-mail notification's body.

Modify

Used to change Cardholder Options. When clicked, settings can be changed on any form in the Cardholder Options folder.

On the Visit Notification Fields form, allows the user to change the contents and order in the e-mail notification's body.

Help

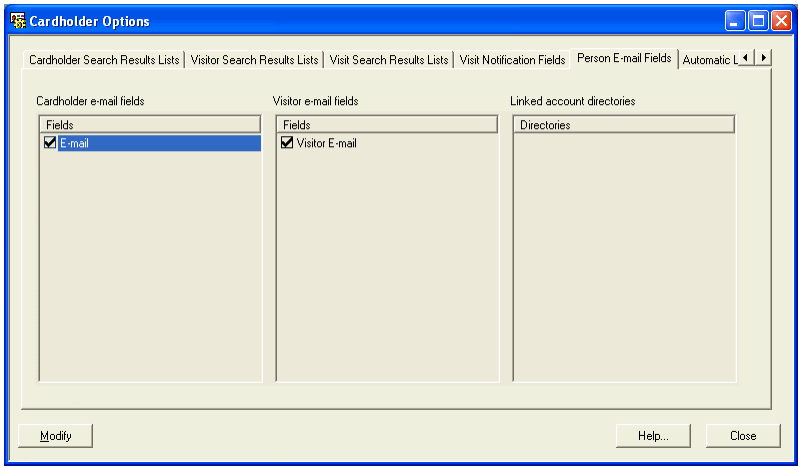
Displays online help for this form.

Close

Closes the Cardholder Options folder.

Person E-mail Fields Form

The Person E-mail Fields form is used to specify which cardholder fields, visitor fields, or linked directories to check when an e-mail notification is sent. On the Person E-mail Fields form, person refers to a cardholder or a visitor.



Cardholder e-mail fields

The check boxes listed in the Cardholder e-mail fields listing window are configured in FormsDesigner. All fields in the Cardholder form with the **vCard** setting of "Internet Email" are displayed. By default, only the **E-mail** field on the Cardholder form has the **vCard** setting of "Internet Email." When an e-mail notification is sent, the selected field will be examined. If an e-mail address has been entered for the record, an e-mail message will be sent to that address.

For example, by default the **E-mail** check box in the Cardholder e-mail fields listing window is listed and selected. If a visit is scheduled and the **Cardholder for this visit** check box on the E-mail form in the Visits folder is selected, then the **E-mail** field on the Cardholder form in the Cardholders folder for the cardholder being visited will be examined. If an e-mail address is found, then that e-mail address will receive an e-mail notification.

The Cardholder e-mail fields are configured in FormsDesigner. For more information, refer to "Configure Cardholder E-mail Fields" in the FormsDesigner User Guide.

Visitor e-mail fields

The check boxes listed in the Visitor e-mail fields listing window are configured in FormsDesigner. All fields in the Visitor form with the **vCard** setting of "Internet Email" are displayed. By default, only the **E-mail** field on the Visitor form has the **vCard** setting of "Internet Email". When an e-mail notification is sent, the selected field will be examined. If an e-mail address has been entered for the record, an e-mail message will be sent to that address.

For example, by default the **Visitor E-mail** check box in the Visitor e-mail fields listing window is listed and selected. If a visit is scheduled. and the **Visitor for this visit** check box on the E-mail form in the Visits folder is selected, then the **E-mail** field on the Visitor form for the cardholder being visited will be examined. If an e-mail address is found, then that e-mail address will receive an e-mail notification.

The Visitor e-mail fields are configured in FormsDesigner. For more information, refer to "Configure Visitor E-mail Fields" in the FormsDesigner User Guide.

Linked account directories

The check boxes that are listed in the Linked account directories listing window are configured in the Directories folder and in the Cardholders folder. All LDAP and Microsoft Active Directory directories that have a value specified in the **E-mail attribute** field on the Advanced sub-tab in the Directories folder will appear in this listing window. (Only an LDAP or Microsoft Active Directory can have an e-mail attribute defined.)

Modify

Used to change Cardholder Options. When clicked, settings can be changed on any form in the Cardholder Options folder. On the Person E-mail Fields form, allows you to select and deselect cardholder and visitor e-mail fields to examine for e-mail addresses when an e-mail notification is sent. Also allows you to select and deselect linked accounts to examine for e-mail addresses when an e-mail notification is sent.

Help

Displays online help for this form.

Close

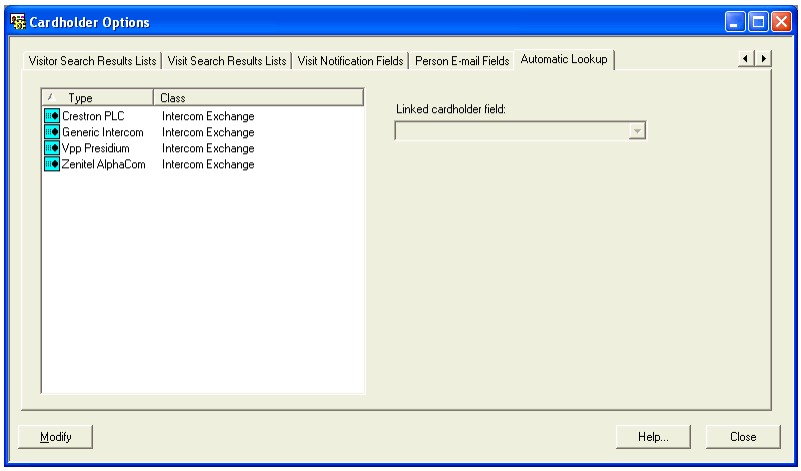
Closes the Cardholder Options folder.

Automatic Lookup Form

The Automatic Lookup Form requires an intercom license to view and/or edit the form. This form is designed to work in conjunction with the Intercom Stations Form on page 1077.The Automatic Lookup form links a cardholder field to a type of intercom panel. You may link any cardholder field (standard or custom) to an intercom panel as long as it is a text field. Field properties, including the type of field, are set in the Field Properties folder of the FormsDesigner application.

The Intercom Stations form links the cardholder field to an intercom station.

Note: Be sure to link a cardholder field to an intercom panel before you link the cardholder field to an intercom station.



Intercom panel type and class listing window

Displays the intercom panel types available. The types of panels that display are based on your intercom license.

Linked cardholder field

Choose the cardholder field you want linked to the intercom type. The drop-down list includes all standard and customized cardholder text fields.

Modify

Used to change cardholder options. When clicked, settings can be changed on any form in the Cardholder Options folder.

Help

Displays online help for this form.

Close

Closes the Cardholder Options folder.

Cardholder Options Folder Procedures

Use the following procedures on this form.

Configure Cardholder Options

1. On the General Cardholder Options tab, click [Modify].
2. Specify the maximum active badges per cardholder.
3. Decide whether or not you wish to have thumbnails created for cardholder photos. If you do, select the **Create/save photo thumbnails** check box.
4. Choose the badge PIN code generation parameters.
5. Choose the precision access mode if it applies to you, or leave it as the default, “None”.
6. If you want inactive badges to be assigned a different badge status, indicate the parameters in the Use or lose badge section.
   a. In the **Number of days** field, enter the number of consecutive days of badge inactivity after which badges will be assigned the badge status indicated in the **New badge status** field. A value of zero disables the use or lose badge feature.
   b. In the **New badge status** field, enter the badge status that will be assigned to badges when the **Number of days** value has been exceeded.

   IMPORTANT: Use or Lose Badge functionality relies on Last Location transaction data. If Use or Lose Badge is enabled on an Enterprise system, Last Location information must be exchanged using Replicator at least twice a day. For more information, refer to Replicator Schedule Form in the Replication Administration User Guide.
7. If you want to change the status of active badges when the deactivate date passes, choose the new badge status from the **After deactivate date, New badge status** drop-down.

Note: For information on the relationship between the use or lose badge settings (configured here) and use or lose badge type settings (configured in the Badge Types folder), refer to Deactivation Settings Form on page 281.

8. Select the **Use time** check box if you want to specify both date and time for the badge activation/deactivation date.

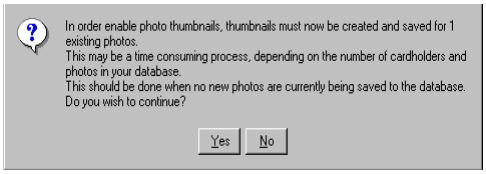
Notes: When this check box is selected, the “Date and time” option will become available for selection in the **Store expiration date** and **Store activation date** drop-down lists on the Options sub-tab on the forms in the Access Panels folder in the System Administration application. Note that only Lenel controllers can use time with badge activation and deactivation dates. For all other controllers, the time will always default to midnight.

Also, when this check box is selected, additional time controls will appear on the Badge form in the Cardholders folder. Modifications to this layout may be needed to properly handle these additional controls. Badge form layout modifications can be made in the FormsDesigner application. For more information, refer to the FormsDesigner User Guide.

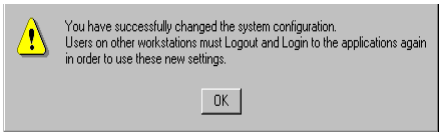
9. For date and time badge activation and deactivation purposes, the Linkage Server examines and updates temporary access levels several times a day (to determine if a badge needs to be added to or removed from a panel). By default, the temporary access levels are examined and updated every 30 minutes. If you would like to change the default, select another value from the **Granularity** drop-down list.

   IMPORTANT: Reducing the temporary access level granularity below the default setting (30 minutes) may impact system performance. (Because temporary access level processing will be performed more frequently, more resources may be consumed.)

10. If you selected the **Create/Save Photo Thumbnails** check box, and if there are currently cardholder records in the database, a message similar to the following will be displayed:



11. Click [Yes] to generate thumbnails for the existing cardholder photos, or [No] to cancel the request and return to the form.
12. If you have made changes using this form, the following message will be displayed:



As the message indicates, any users that are currently accessing the system must log out then log in again.

Configure ID Allocation

If you want to configure the ID allocation for every badge type, complete the following procedures. If you want to configure the ID allocation for a specific badge type refer to the Badge Types folder, Badge ID Allocation form.

Note: Changes made to the Badge ID Allocation form in the Badge Types folder override settings on the Badge ID Allocation form in the Cardholder Options folder.

1. Select ***Cardholder Options*** form the ***Administration*** menu or select the appropriate toolbar button.
2. On the Badge ID Allocation tab click [Modify].
3. On the ID Allocation sub-tab:
   a. Select the method you will use to generate badge IDs from the **Generate Badge ID** drop-down list.
   b. Select the **Allow Edit of Badge ID** check box if you want badge operators, with the proper permission, to modify badge IDs. If badge ID is generated From 'Cardholder ID' or Manual Entry, badge IDs can be edited BEFORE printing. Users with the **Can edit ID/issue/type after printing permission** can also edit badge IDs AFTER printing.
   c. Enter the number of the first issue code. Typically, this value is zero.
   d. Select the **Auto-Increment Issue Code** check box if you want the issue code to automatically increment when a new badge is created.
   e. If you selected FASC-N for badge ID generation, enter the four-digit codes identifying the government agency and system issuing the credential. The agency and system codes are encoded on smart cards and become part of the OnGuard badge ID. Select the user-defined fields that will be populated with the agency code, system code and credential ID.
4. On the ID Ranges sub-tab:
   a. Enter the numeric values in the **First ID** and **ID count** fields. The **Last ID** field automatically populates.
   b. Click [Add]. If [Add] is not enabled, you did not enter a valid range.

5. Click [OK].

Add a Fixed ID Range

1. Open the Cardholder Options folder.
2. Click the Badge ID Allocation tab.
3. Click [Modify].
4. On the ID Allocation sub-tab:
   a. In the **Generate Badge ID** field, select the method you will use to generate badge IDs. The **Generate Badge ID** field must be set to either 'Manual Entry' or 'Automatic' to add a fixed ID range.
   b. Depending on your selection, the default settings displayed for the **Allow Edit of Badge ID** and **Auto-Increment Issue Code** check boxes will automatically change. If the check box is enabled, you can change it if you need to.
   c. In the **First Issue Code** field, enter the number that will be used as the first issue code.
5. On the ID Ranges sub-tab:
   a. Enter numeric values in the **First ID** and **ID count** fields. The **Last ID** field will automatically populates.
   b. If you have entered a valid range, the [Add] button will be enabled. Click [Add]. If the fixed ID range does not conflict with a range that already exists, it will be added to the Allocated ranges listing window.
6. Click [OK].

Modify a Fixed ID Range

1. Open the Cardholder Options folder.
2. Click the Badge ID Allocation tab.
3. Click [Modify].
4. On the ID Ranges sub-tab:
   a. In the Allocated Ranges listing window, select the fixed ID range to be modified. The values associated with the selected fixed ID range will be displayed in the **First ID**, **ID count**, and **Last ID** fields.
   b. Make changes to any of those three fields that you want to change.
   c. Click [Modify].
5. Click [OK].

Delete a Fixed ID Range

1. Open the Cardholder Options folder.
2. Click the Badge ID Allocation tab.
3. Click [Modify].
4. On the ID Ranges sub-tab:
   a. In the Allocated ranges listing window, select the fixed ID range to be deleted.
   b. Click [Delete]. The fixed ID range will be deleted without any confirmation.
5. Click [OK].

Configure System-wide Visit Options

System-wide visit sign in options can be configured in System Administration or ID CredentialCenter, but not in Visitor Management. To configure the options that will be available for visit sign in and sign out in System Administration, ID CredentialCenter, and Visitor Management:

1. In ID CredentialCenter or System Administration, select the ***Administration > Cardholder Options*** menu option.
2. On the Visits tab, click [Modify].
3. In the **Default visit time in** and **Default visit time out** fields, select the time that visits will start and end. These are the default values that will appear in the **Scheduled time in** and **Scheduled time out** fields on the Visit form.
4. Specify the default refresh rate (in minutes). This *refresh rate* is the frequency the database is queried for changes, and affects the results of visit searches based on status (e.g., the "Scheduled, future", "Scheduled, late", and "Active" status).
5. Select the visit options you wish to use.

Note: If the title of the check box you are selecting has the word "default" in it, you are setting a default value and badge operators can change these default values in the Visits folder. Otherwise, you are enabling a feature which cannot be changed by badge operators.

   a. Select the **Sign in now by default** check box if you want visits to automatically be signed in and printed when they are added to the system. Badge operators can override the default setting by deselecting the **Sign In Now** check box on the Visits form.
   b. Select the **Allow disposable badge printing** check box to enable disposable badge printing. In addition, the disposable badge type should be assigned a printer.
   c. Select the **Allow access control badge assignment** check box to allow an existing access control badge to be assigned to a visitor when a visit is added. This option must be selected if you want badge operators to assign access control badges from the Sign In Visit(s) window.
   d. Select the **Allow e-mail notification** check box to enable e-mail notification.

Note: E-mail notification requires the GOS module to be configured and running. For more information, refer to the Global Output Devices Folder chapter in the System Administration User Guide.

   e. Select the **Include host's e-mail by default** and/or **Include visitor's e-mail by default** check box if you want the host or visitor to be included in the e-mail notification.
   f. Select the **Synchronize active badges and active visits** check box to automatically update badge activation/deactivation dates if changes are made to the scheduled time in/out fields. Select the **Prompt user** check box if you want badge operators to decide whether badges activation/deactivation dates are updated. For more information, refer to the Cardholder Options Folder chapter in the System Administration User Guide.
   g. In the **Badge status for sign out** drop-down list, select the badge status when a visitor signs out.
   h. Click [OK].

Synchronize Active Badges with Active Visits

This option synchronizes the badge activation and deactivation date with the visit time in and visit time out. A visitor's badge is activated at the beginning of the day the visit is scheduled for and deactivated at the end of the day that the visit is scheduled for.

For example, the badge of a visitor who is scheduled to visit from 8 a.m. to 5 p.m. on Wednesday would be activated on Tuesday at midnight and would be deactivated on Wednesday at midnight. If the visitor arrives and is signed in, and then visit's scheduled time out is changed to Friday at 5 p.m., this is where the visit synchronization feature would become important. If the synchronization feature is enabled, then the deactivation date for the badge would be changed to match the new scheduled time out, and would be deactivated at midnight on Friday. If the synchronization feature is disabled, then the original deactivation date, which was Wednesday at midnight, would still be used.

Active badges can be synchronized with active visits when:

- An active visit (one that is signed in) is changed. For example, the person was scheduled to leave at 3 p.m., but you change the scheduled time out to 5 p.m. The example given above falls into this category.
- Multiple active badges are assigned to a visitor for a visit, and an active visit is signed out. (This doesn't happen often because usually a visitor only has one active badge.)

Whether active badges are synchronized with active visits depends on the settings for the **Synchronize active badges and active visits** and **Prompt user** check boxes on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter.The following table describes each possible combination of settings.

Summary of Active Badge and Active Visit Synchronization Settings

Synchronize active badges and active visits check box selected?	Prompt user check box selected?	How synchronize feature works
Yes	Yes	By default, both of these check boxes are selected. Active badges will be synchronized with active visits, and you will be prompted before the synchronization occurs. The prompt gives you a clear understanding of what is being synchronized, and allows you to choose which badges will be synchronized if the visitor has multiple active badges.
Yes	No	All active badges and active visits will be synchronized, and you will not be prompted when they are synchronized. If a visitor has multiple active badges, you will not be able to choose which active badges get synchronized; they will all get synchronized.
No	No	Active badges and active visits will not be synchronized. For example, if the scheduled time out is changed for a visitor who is signed in, the deactivation date of the active badge will not be updated to match the new scheduled time out.

To change the visit synchronization settings:

1. In ID CredentialCenter or System Administration, select the ***Administration*** > ***Cardholder Options*** menu option.
2. Click the Visits tab.
3. Click [Modify].
4. Refer to Summary of Active Badge and Active Visit Synchronization Settings on page 446 to determine which synchronization settings you wish to use.
   a. Select or deselect the **Synchronize active badges and active visits** check box.
   b. Select or deselect the **Prompt user** check box.

5. Click [OK].

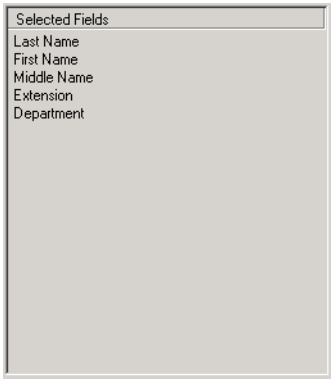
Configure the Cardholder Search Results Lists

The columns displayed on the Select People window and the Area Access Manager main window, as well as the Select Host Wizard: Select window in the Visits folder can be changed using System Administration. To change the columns displayed:

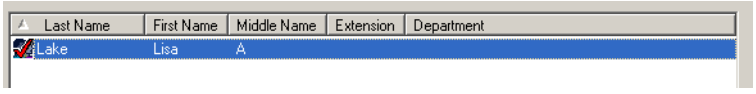
1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Cardholder Options***.
2. Click the Cardholder Search Results Lists tab.
3. Click [Modify].
4. In the Fields column, click on the field you want to be displayed in the Area Access Manager main window, the Select People window, and the Select Host Wizard: Select window. (Only one field can be selected at a time.)
5. Click the button to add the selected field to the list of fields that will be displayed.
6. Repeat steps 4 and 5 until all fields to be displayed are listed in the Selected Fields column.

Notes: The order that the fields are listed in the Selected Fields column is the order that the columns will be displayed in, from left to right, in the Area Access Manager main window, the Select People window, and the Select Host Wizard: Select window.

For example, if the selected Fields listing window on the Cardholder Search Results Lists form looks like this:



then the columns in the Select Host Wizard: Select window will be laid out like this:



7. Select a field in the Selected Fields column, then:
   - Click the button to move the selected field one position to the left, or
   - Click the button to move the selected field one position to the right.
8. Click [OK].

Configure the Visitor Search Results Lists

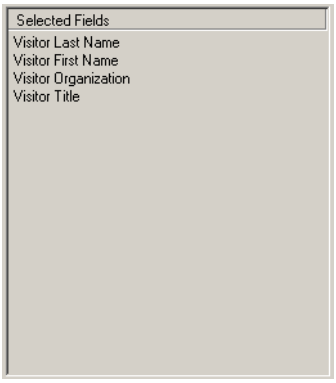
The columns displayed on the Select Visitor Wizard: Select window in the Visits folder can be changed using System Administration. To change the columns displayed:

1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Cardholder Options***.
2. Click the Visitor Search Results Lists tab.
3. Click [Modify].
4. In the Fields column, click on the field you want to be displayed in the Select Visitor Wizard: Select window. (Only one field can be selected at a time.)
5. Click the

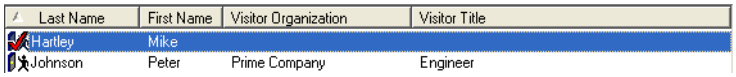
button to add the selected field to the list of fields that will be displayed.
6. Repeat steps 4 and 5 until all fields to be displayed are listed in the Selected Fields column.

Notes: The order that the fields are listed in the Selected Fields column is the order that the columns will be displayed in, from left to right, in the Select Visitor Wizard: Select window.

For example, if the Selected Fields listing window on the Visitor Search Results Lists form looks like this:



then the columns in the Select Visitor Wizard: Select window will be laid out like this:



7. Select a field in the Selected Fields column, then:
   - Click the button to move the selected field one position to the left, or
   - Click the button to move the selected field one position to the right.
8. Click [OK].

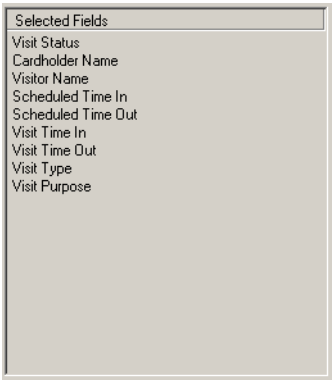
Configure the Visit Search Results Lists

The columns displayed in the Visits listing window in the Visits folder can be changed using System Administration. To change the columns displayed:

1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Cardholder Options***.
2. Click the Visit Search Results Lists tab.
3. Click [Modify].
4. In the Fields column, click on the field you want to be displayed in the Select Visitor Wizard: Select window. (Only one field can be selected at a time.)
5. Click the button to add the selected field to the list of fields that will be displayed.
6. Repeat steps 4 and 5 until all fields to be displayed are listed in the Selected Fields column.

Notes: The order that the fields are listed in the Selected Fields column is the order that the columns will be displayed in, from left to right, in the Visits listing window in the Visits folder.

For example, if the Selected Fields listing window on the Visit Search Results Lists form looks like this:



then the columns in the Visits listing window in the Visits folder will be laid out like this:

7. Select a field in the Selected Fields column, then:
   a. Click the button to move the selected field one position to the left, or
   b. Click the button to move the selected field one position to the right.
8. Click [OK].

Configure the Visit Notification Fields

The information that is included in visit notification e-mails can be changed using System Administration. To change the information sent:

1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Cardholder Options***.
2. Click the Visit Notification Lists tab.
3. Click [Modify].

4. In the Fields column, click on the field you want to be displayed in the Select Visitor Wizard: Select window. (Only one field can be selected at a time.)
5. Click the button to add the selected field to the list of fields that will be displayed.
6. Repeat steps 4 and 5 until all fields to be displayed are listed in the Selected Fields column.

Note: The order that the fields are listed in the Selected Fields column is the order that the information will be included in the visit notification e-mail.

7. Select a field in the Selected Fields column, then:
   a. Click the button to move the selected field one position to the left, or
   b. Click the button to move the selected field one position to the right.
8. Click [OK].

Modify the Person E-mail Fields

The person e-mail fields consist of the cardholder and visitor e-mail fields, as well as linked directory accounts. Both the cardholder e-mail fields and the Visitor e-mail fields are configured in FormsDesigner. To modify the person e-mail fields:

1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Cardholder Options***.
2. Click the Person E-mail Fields tab.
3. Click [Modify].
4. In the Cardholder e-mail fields listing window, select the field(s) in the Cardholders folder from which you want to get e-mail addresses. By default, the “E-mail” entry is selected, which means that when the **Cardholder for this visit** check box is selected on the E-mail form in the Visits folder, and an e-mail notification is sent, the e-mail address that will be sent an e-mail notification is the e-mail address that is listed in the **E-mail** field on the Cardholder form in the Cardholders folder.

Note: The Cardholder e-mail fields are configured in FormsDesigner. For more information, refer to “Configure Cardholder E-mail Fields” in the FormsDesigner User Guide.

5. In the Visitor e-mail fields listing window, select the field(s) in the Visitor folder from which you want to get e-mail addresses. By default, the “Visitor E-mail” entry is selected, which means that when the **Visitor for this visit** check box is selected on the E-mail form in the Visits folder, and an e-mail notification is sent, the e-mail address that will be sent an e-mail notification is the e-mail address that is listed in the **E-mail** field on the Visitor form in the Cardholder folder.

Note: The Visitor e-mail fields are configured in FormsDesigner. For more information, refer to “Configure Visitor E-mail Fields” in the FormsDesigner User Guide.

6. In the Linked account directories listing window, all LDAP and Microsoft Active Directory directories that have a value specified in the **E-mail attribute** field on the Advanced sub-tab in the Directories folder will be listed. (Only an LDAP or Microsoft Active Directory can have an e-mail attribute defined.) To add a directory, refer to “Add a Directory” in the Directories Folder chapter in the System Administration User Guide.

Notes: The linked account directories will be checked in addition to the Cardholder e-mail fields. If a cardholder has a different address specified in their cardholder record than

the e-mail address that the linked directory is using, an e-mail notification will be sent to both addresses. This only occurs if the **Cardholder for this visit** check box is selected on the E-mail form in the Visits folder.

The linked account directories will be checked in addition to the Visitor e-mail fields. If a visitor has a different address specified in their visitor record than the e-mail address that the linked directory is using, an e-mail notification will be sent to both addresses. This only occurs if the **Visitor for this visit** check box is selected on the E-mail form in the Visits folder.

7. Click [OK].

CHAPTER 18

Segments Folder

The Segments folder contains forms with which you can activate the segmentation feature. The folder contains the Segment Options form. Two additional forms, the Segments form, and the Segment Group form display only if your installation uses segmentation.

This folder displays when you select ***Segments*** from the ***Administration*** menu or select the Segments toolbar button.

Toolbar Shortcut

Segments Folder Procedures

Use the following procedures for this folder.

Log Into the Application as a User with Access to All Segments

1. On the log on screen, enter the user name and password for an account that has access to all segments.
2. Click [OK].
3. The Select Segment window will prompt you to select a segment to log into from a list of all currently defined segments. You can either:
   - Choose the default, “Access all segment assignments”, or
   - Select “Apply segment filter” and select one specific segment to work in

     If you choose a particular segment, during that session your user interface will be the user interface of a regular Segment User for the specified segment. The application will display only records that are contained in the selected segment. This is convenient if you will be configuring within one segment only for a session.
4. The main window will be presented. If you logged into a specific segment, the name of that segment will be listed in the application’s title bar.

Add Segments to Your Installation

• WARNING! • It is CRITICAL that you first think about how you want your system to function, and then define the segments and select the appropriate options for each. This must be done before you attempt to put your segmented system into use.

Segments are added using the Segments form of the Segments folder. Features available by using the New Segment Wizard include:

- Copy objects from an existing segment to the new segment you're adding
- Assign selected access panels to the new segment
- Perform an automatic full download to each of the selected access panels after they're moved to the new segment

There are two situations in which this form is used:

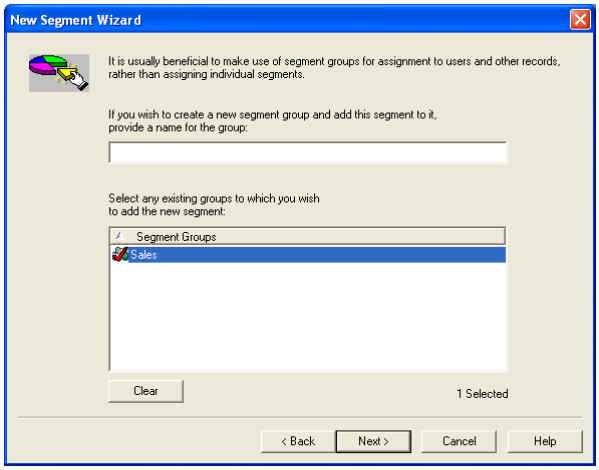
- You want to move existing Access Panels to the new segment.
- You don't want to move existing Access Panels to the new segment, but you do want to copy some objects (e.g., Holidays and Timezones) to the new segment for convenience.

Additional features available by using the New Segment Wizard include:

- Automatically adding the segment to a new or existing Segment Group (this is recommended)
- Optionally clean up the source segment by removing any access levels which no longer have readers or access groups that no longer have levels after panels have been moved
- Optionally prefix or append text to the names of records when copying

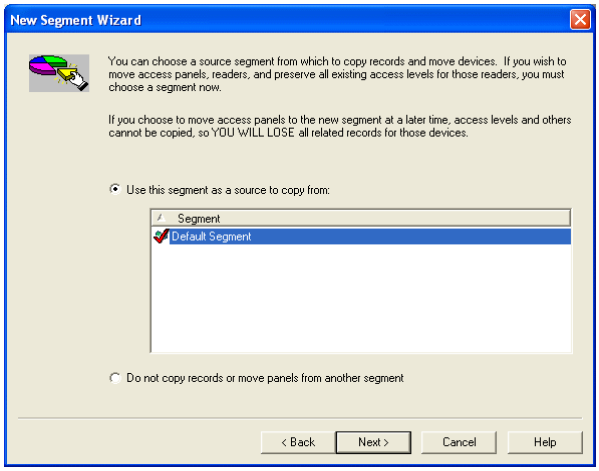
To add a segment to your installation:

1. Log in as a user who has access to all segments and select the "Access all segment assignments" option in the Select Segment window.
2. Select the ***Administration*** **>** ***Segments*** menu option.
3. On the Segments form in the Segments folder, click [Add].
4. The New Segment Wizard opens. Enter a unique, descriptive name for the segment you're adding.
5. Click [Next].
6. The wizard proceeds. Skip this step if you do not wish to use segment groups. Otherwise, do the following:
   a. If you want to create a new segment group for the segment, type the name you want to use in the first blank field.
   b. If you want to add the segment to existing segment groups, select them in the Segment groups listing window.

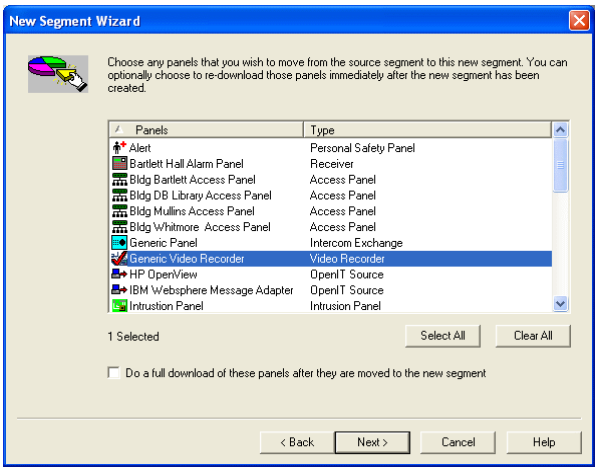


7. Click [Next].
8. The wizard proceeds.
   a. Select either the **Use segment as a source to copy from** or the **Do not copy records or move panels from another segment** radio button.
   b. If you selected **Use segment as a source to copy from**, click on the segment you wish to copy from in the Segment listing window. A red checkmark will appear over the icon of the selected segment.

Note: It's best if all selected access panels are currently in the same segment that you choose in the Segment listing window of the **Use this segment as a source to copy from** option. Then you would choose to copy all records from that segment. Although you can move access panels from other segments also, all links for those access panels will be lost, since you can use this window to copy system records from only one segment.



9. Click [Next].
10. The wizard proceeds.
    a. In the listing window, select any panel(s) you wish to move from the source segment to the new segment.
       - If you wish to select all the panels listed, click [Select All].
       - If you wish to deselect all panels listed, click [Clear All].



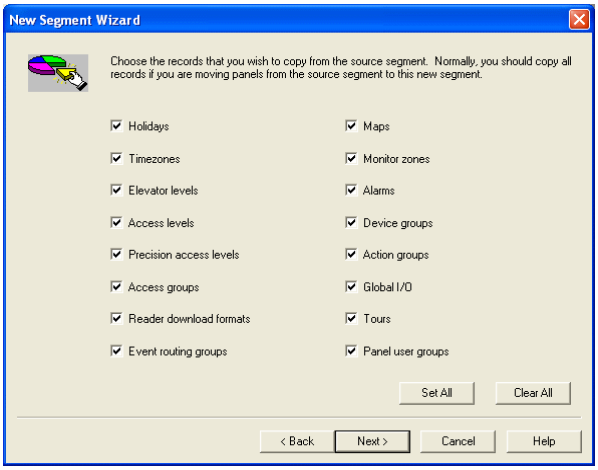
b. Select the **Do a full download of these panels after they are moved to the new segment** check box to perform a full download to each of the selected access panels automatically after the panels are moved to the new segment. This ensures that the panels are updated to include the object records that you selected for copying.

c. If you do not select the **Do a full download of these panels after they are moved to the new segment** check box, you should manually perform a full download to the affected panels after they've been moved to the new segment. The wizard will display the following warning message (after you click [Next]) to warn you of this.

d. If the warning message above is displayed, click [OK].

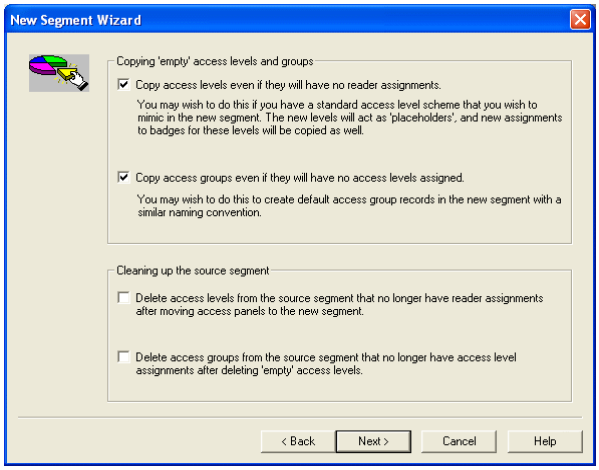
11. Click [Next].

12. The wizard proceeds. Select the records you wish to copy from the source segment.

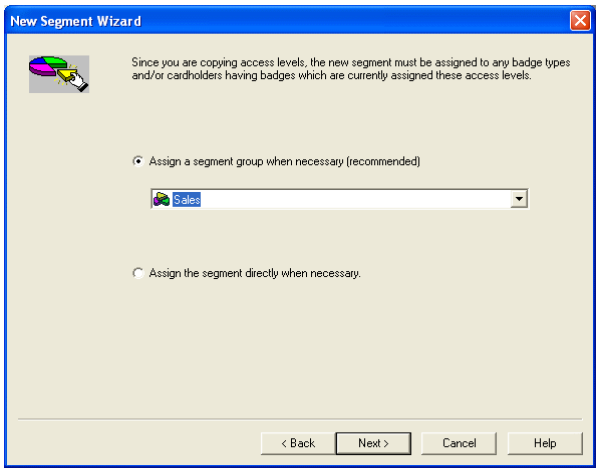


13. Click [Next].

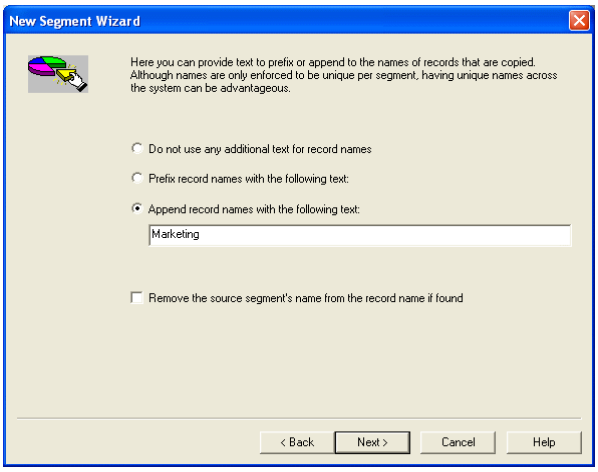
14. Select the each of the options you desire in the Copying empty access levels and groups and Cleaning up the source segment sections.



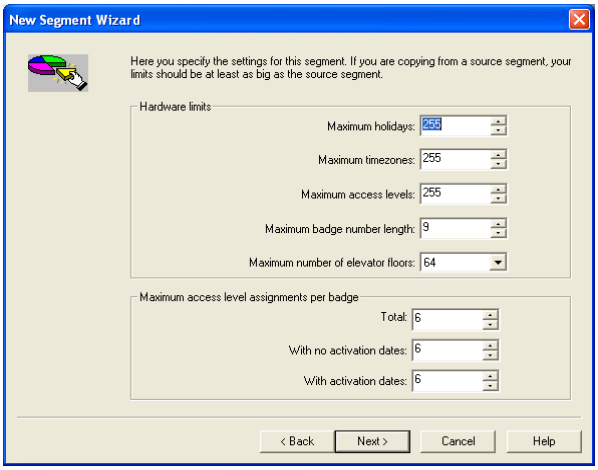
15. Click [Next].
16. The Wizard proceeds.



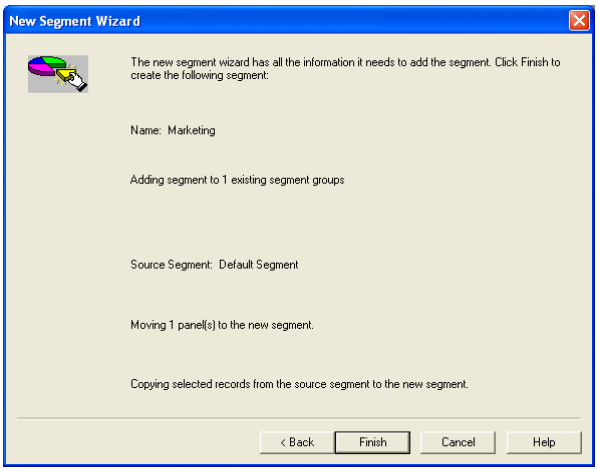
17. Click [Next].
18. The wizard proceeds.
    a. Select an option for the text to prefix or append to the names of the records that are copied.
    b. Select the **Remove the source segment's name from the record name if found** if you wish.



19. Click [Next].
20. The wizard proceeds. Make selections in the Hardware Limits and Access Level Assignments sections. (These properties can be modified after the segment has been created.)



21. Click [Next].
22. The wizard proceeds to its final screen, and a summary of the characteristics of the new segment is displayed. Make sure that these characteristics are what you want, then click [Finish].



23. A status window will appear and get updated as the segment is added. Once the segment has been added, it will automatically appear in the Segment listing window on the Segments form in the Segments folder.

Notes About the New Segment Wizard

- Because access panels are segmented, all other segmented objects that are related to access panels are affected when you reassign an access panel to a different segment. For this reason, you are strongly encouraged to take this ONE opportunity (since this option is only offered in the New Segment Wizard when you're creating a segment) to copy all related records for the panels to be moved to the new segment.

Note: If at a later time you wish to move an access panel to the new segment, all existing links to other records such as Access Level assignments (reader + timezone/elevator level), Badge/Access Level assignments, Monitoring Zone assignments and Map items, etc. will be PERMANENTLY LOST.

- For records that contain definitions that include access panel-related items (e.g., maps, monitor zones, access levels), only the definitions for hardware attached to access panels that you are moving will get moved. For example: You currently have "Access Panel A" and "Access Panel B" in "Segment 1". "My Access Level" contains reader/timezone assignments for readers on both "Access Panel A" and "Access Panel B". You then add "Segment 2", choose to copy access levels, and move "Access Panel B" to the new "Segment 2". "My Access Level" will get copied to "Segment 2", and the reader assignments for readers on "Access Panel B" will get moved to the access level definition in "Segment 2". The level in "Segment 1" will be left only with assignments for readers on "Access Panel A".

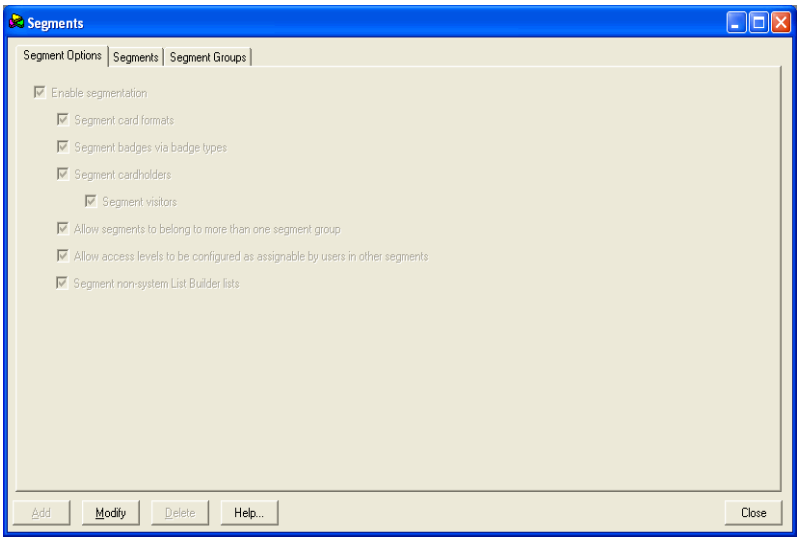
Segment Options Form

The Segment Options form is used to:

- Activate the Segmentation feature
- Select additional options for segmenting card formats, segmenting badges via badge types, and allowing segments to belong to more than one segment group (These options are only enabled for selection after the **Enable segmentation** check box has been checked and segmentation has been enabled.)

IMPORTANT: It is advisable to determine and configure segment options prior to entering any data into your system.

Note: This form displays on segmented and unsegmented systems. The Modify button on this form is disabled if a segment filter is chosen at login time.



Enable Segmentation

Activates Segmentation. This also enables the **Segment card formats**, **Segment badges via badge types**, **Segment cardholders**, **Allow segments to belong to more than one segment group**, and **Allow access levels to be configured as assignable by users in other segments** check boxes.

Segment card formats

If selected, card format segmentation is enabled. In card format segmentation, a card format can belong to <All Segments> (system-wide), one segment, or many segments.

Segment badges via badge types

If selected, badge type segmentation is enabled. In badge type segmentation, a card format can belong to <All Segments> (system-wide), one segment, or many segments. When badge types are segmented, cardholders' badges are in effect segmented as well, by virtue of their badge type. A badge type's segment(s) determine:

- Which default access groups can be assigned to the badge type.
- Which magnetic card formats can be assigned to the badge type, if card formats are also segmented.
- Which users can see and edit the badge type. A user must have at least one segment in common with a badge type in order to view it, and must have access to the "Primary Segment" of the badge type (described later) in order to edit it.
- Which badge types a user can assign to a badge. A user must have access to the badge type's "Primary Segment" in order to assign it to a new or existing badge.
- Which badges a user can see. A user must have at least one segment in common with a badge type in order to see badges of that type. However, unless they have access to the badge's primary segment, they cannot modify or delete the badge; they can only assign and remove access levels to it.
- Which access levels a badge can have assigned to it. For example, even if a user has access to segments A, B and C, if the badge's type only belongs to segment A, only access levels in segment A can be assigned to the badge.

Segment cardholders

If selected, cardholders can be segmented. This also enables the **Segment visitors** check box to be selected.

Segment visitors

If selected, visitors can be segmented. Note that **Segment cardholders** must be selected before **Segment visitors** can be selected.

Allow segments to belong to more than one segment group

Segment groups can be assigned to users and badge types.

If not selected, a segment can only belong to one segment group.

If selected, a segment can belong to more than one segment group.

For example, consider a system that has segments A, B, C, and D. Segments A and B might belong to one segment group, while segments C and D belong to another segment group. Segments A, B, C, and D can be assigned to some third segment group if desired.

Allow access levels to be configured as assignable by users in other segments

If selected, the Access Level Additional Segments form will be displayed in the Access Levels/ Assets folder. This form allows users to specify additional segments whose users are allowed to assign a level. When this option is enabled, any user with permission to modify access levels can assign additional segments to a level.

Segment non-system List Builder lists

If selected, List Builder entries are shown across all regional nodes of the Enterprise system regardless of what List Builder entries are assigned to what node. This is done to avoid duplicate entries at the master node. Each node may only use and modify those List Builder entries assigned to them.

Add

This button is not used.

Modify

Changes any of the segmentation options on this form. If the **Enable segmentation** check box is selected, it cannot be deselected. The Modify button is disabled if a segment filter is chosen at login time

Delete

This button is not used.

Help

Displays online help for this form.

Close

Closes the Segments folder.

Segment Options Form Procedures

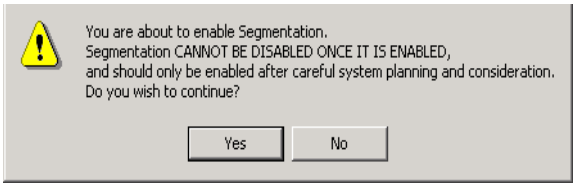
Use the following procedures on this form.

Configure an Installation to Use Segmentation

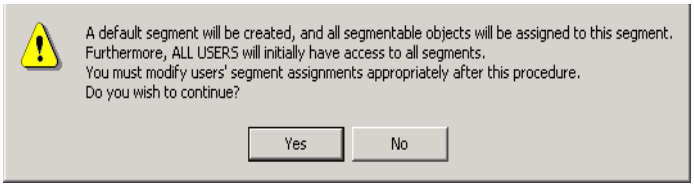
• WARNING! • Once the Segmentation feature is enabled, it CANNOT be disabled. For this reason, segmentation should be enabled only after careful system planning and consideration.

To enable segmentation:

1. From the ***Administration*** menu, select ***Segments***, or click the Segments toolbar button.
2. On the Segment Options form, click [Modify].
3. Select the **Enable segmentation** check box.
4. Click [OK]. The following message will be displayed:



5. Do one of the following:
   - If you don't want to enable segmentation, click [No]. This returns you to the Segment Options form.
   - Click [Yes] to proceed. The following message will then be displayed:



6. Do one of the following:
   - If you don't want to enable segmentation, click [No]. This returns you to the Segment Options form.
   - Click [Yes] to enable segmentation.

As the message indicates, several things happen during this conversion:

- A default segment is created, and all segmentable records are allocated to this segment.
- A Segments form and Segment Groups form are added to the Segments folder to allow you to add, modify, and delete segments and segment groups.
- Any other forms that are open at the moment are closed (this is so they have the proper segmentation controls showing the next time you open them).
- All users are made <All Segments> Users, allowing them to view all segments and to do software configuration from within any segment of choice. Such unrestricted access by all users negates the advantages of using segmentation. Segmented installations have the ability to limit a user to operating within one segment, and it is the job of the System Administrator to define each user's segmentation abilities. For more information, refer to Restrict User Access to Segments on page 352.
- After the initial segmentation setup is complete, you may change the name of the "Default Segment" to another name if desired.

Enable Additional Segmentation Features

After segmentation has been enabled, there are several additional segmentation features available to you. You can choose to segment card formats, segment badges via badge types, and/or allow segments to belong to more than one Segment Group.

To enable any of the above features:

1. From the ***Administration*** menu, select ***Segments***, or click the Segments toolbar button.
2. Click the System Options tab.
3. Click [Modify].
4. In the Segmentation section, select the check box of each additional segmentation features you wish to enable. Choices available include:
   - Segment card formats
   - Segment badges via badge types
   - Segment cardholders
   - Segment visitors
   - Allow segments to belong to more than one segment group
   - Allow access levels to be configured as assignable by users in other segments
5. Click [OK].

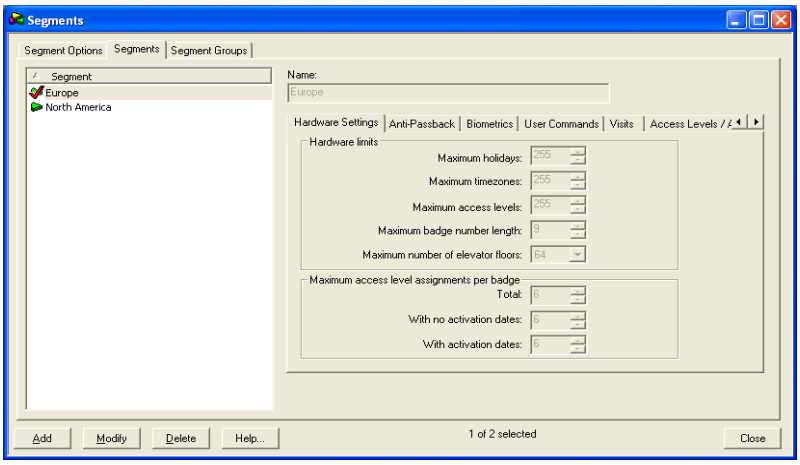
Segments Form (Hardware Settings Sub-tab)

The Hardware Settings sub-tab is used to:

- Specify the maximum number of holidays, timezones, and access levels that can be defined in the system.
- Specify the maximum badge number length.
- Specify the maximum number of standard access levels, temporary access levels, and total access levels that can be assigned to an individual cardholder badge.

It is advisable to determine and configure Hardware Setting options prior to entering any data into your system.

Note: This form displays when segmentation is enabled. When segmentation is not enabled, these options are available on the Hardware Settings form in the System Options folder.



Maximum holidays

If you are using Lenel access panels, choose a value between 20 and 255 to specify the maximum number of holidays that can be defined in the system. The default is 255.

Maximum timezones

If you are using Lenel access panels, choose a value between 127 and 255 to specify the maximum number of timezones that can be defined in the system. The default is 255.

Maximum access levels

If you are using Lenel access panels, choose a value between 255 and 31,999 to specify the maximum number of access levels that can be defined in the system. The default is 255.

Maximum badge number length

Choose a maximum number of digits a badge can be for manual entry of badge IDs. Lenel access panels support a maximum of an 18-digit badge number (maximum value 999,999,999,999,999,999).

Badge IDs require 4 to 8 bytes of memory when stored in access panels, depending on the number of digits in a badge.

- 9 digits or less require 4 bytes
- 10-12 digits require 5 bytes
- 13-14 digits require 6 bytes
- 15-16 digits require 7 bytes
- 17-18 digits require 8 bytes

Maximum number of elevator floors

Choose a maximum number of elevator floors to correspond with the floors in your building. The maximum number is 128.

Total

Specify the maximum number of access levels that can be assigned to a badge at one time. This includes both standard and temporary access levels. If you are using Lenel access panels, the maximum allowed is 32. If you reduce this number, you will be prompted that the application must proceed with a validation of each badge in the database to ensure that there are currently no badges that have more access level assignments than the value you are attempting to set. If there exist badges that have too many assignments, a message box will display the badge ID that is in

violation. If you wish to proceed, you must search up the badge in the Cardholders folder and reduce its access level assignments.

With no activation dates

Specify the maximum number of standard access levels that can be assigned to a badge at one time. *Standard access assignments* are regular assignments with no activate/deactivate date. In most cases, this will be set equal to the number entered in the **Total** field. If you are using Lenel access panels, the maximum allowed is 32. This number cannot exceed the value in the **Total** field.

With activation dates

Specify the maximum number of temporary access level assignments that a badge can have. In most cases, this will be set equal to the number entered in the **Total** field. A *temporary access level* assignment is one that has been assigned an activate date, a deactivate date, or both. If you are using Lenel access panels, the maximum allowed is 32. This number cannot exceed the value in the **Total** field.

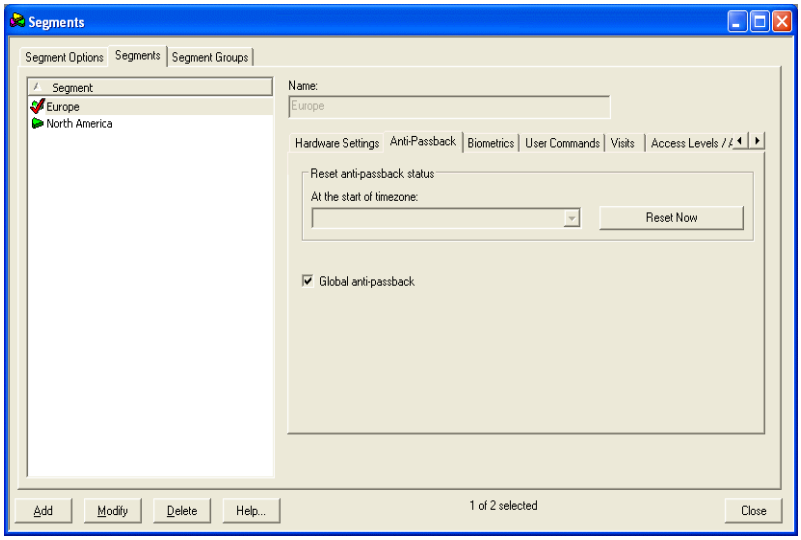
Segments Form (Anti-Passback Sub-tab)

The Anti-Passback sub-tab is used to:

- Specify when to reset the anti-passback status for users associated with a given segment.
- Select whether the system will use global anti-passback.

It is advisable to determine and configure Anti-Passback options prior to entering any data into your system.

Note: This form displays when segmentation is enabled. When segmentation is not enabled, these options are available on the Anti-Passback form in the System Options folder.



At the start of timezone

Cards used in anti-passback readers will be made usable again at the beginning of the selected timezone. Choices include the names of all currently defined timezones.

Example: In situations where people may have left an area without swiping their cards through anti-passback readers (perhaps at the end of the work day) this insures that they will be allowed to reenter properly the next day.

Reset Now

This button is intended for use when a cardholder has committed an anti-passback violation and can't get into or out of a particular area.

If you click this button on a non-segmented system, a confirmation message that says "Are you sure you wish to reset global anti-passback status?" will be displayed. If you click [Yes], cards used in anti-passback readers will become usable again immediately.

If you click this button on a segmented system, a confirmation message that says "Are you sure you wish to reset global anti-passback status for segment *<segment name>*?" will be displayed. If you click the [Yes] button, cards used in anti-passback readers in the selected segment will become usable again immediately.

Global anti-passback

If selected, global anti-passback features can be used. When this check box is not selected the Areas folder only contains the Anti-Passback Areas form. When this check box is selected, the Areas folder contains the Anti-Passback Areas, Associated Safe Locations, Associated Inside Areas, and Muster Reporting forms.

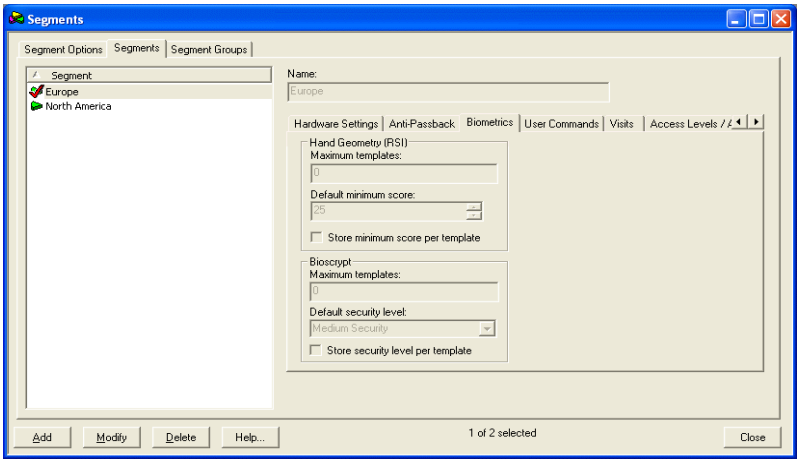
Segments Form (Biometrics Sub-tab)

The Biometrics sub-tab is used to:

- Specify Hand Geometry biometric settings including maximum templates, default minimum score, and whether to store the minimum score per template.
- Specify Bioscrypt biometric settings including maximum templates, default minimum score, and whether to store the minimum score per template.

It is advisable to determine and configure biometric options prior to entering any data into your system.

Note: This form displays when segmentation is enabled. When segmentation is not enabled, these options are available on the Biometrics form in the System Options folder.



Hand Geometry

Maximum templates

Enter the maximum number of templates that can be downloaded to the controller. The maximum number of templates is limited by the amount of free space on the controller. Each hand print template occupies 20 bytes. A total of 22 bytes are required per template if individual scores are stored with the template. Additional memory is required to enable HandKey support.For more information, refer to LNL-2000 (Options Sub-tab) on page 589.

Default minimum score

Choose the minimum score required to accept a template match between the access control reader and the template in the database.The lower the specified score, the closer the match must be during the verification process. Scores range from 1-255, with the default score being 25.

Store minimum score per template

Select this check box if you want minimum acceptance scores to be stored on a per template basis. If this check box is selected and the given template has a minimum acceptance score, the default will be overridden. If not selected, the default will be used.

Bioscrypt

Maximum templates

Enter the maximum number of templates that can be downloaded to the controller. The maximum number of templates is limited by the amount of free space on the controller. Each fingerprint template occupies 362 bytes. Additional bytes are not required if individual scores are stored with the template because of the way the system rounds to the nearest even number. Additional memory is required to enable Bioscrypt support. For more information, refer to LNL-2000 (Options Sub-tab) on page 589.

Default security level

Select the default security level from the drop-down list.

Store security level per template

Select this check box if you want the default security level to be stored on a per template basis. If this check box is selected and the given template has a default security level, the default will be overridden. If not selected, the default will be used.

Modify

Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help

Displays online help information for this form.

Close

Closes the System Options folder.

Biometrics Sub-tab Procedures

The following procedures can be performed on this tab.

Configure Biometrics

Complete this procedure to configure the maximum number of templates that can be downloaded to the access panel, as well as the minimum score necessary for template verification.

Note: The default number of templates that can be downloaded to the access panel is zero. Therefore, you must change the default value. If you do not change the default value, data will not be sent to the access panel and the controller capacity status will not display in Alarm Monitoring.

1. From the ***Administration*** menu, select ***Segments***, or click the Segments toolbar button.
2. Click the Segments tab. Click the Biometrics sub-tab.
3. Click [Modify].
4. If you are working with HandKey:
   a. Enter the maximum number of templates to be downloaded to the controller.
   b. Enter the default minimum score required to accept a template match between the template read at the reader and the template stored in the database.

Note: The lower the HandKey score, the closer the match must be during the verification process.

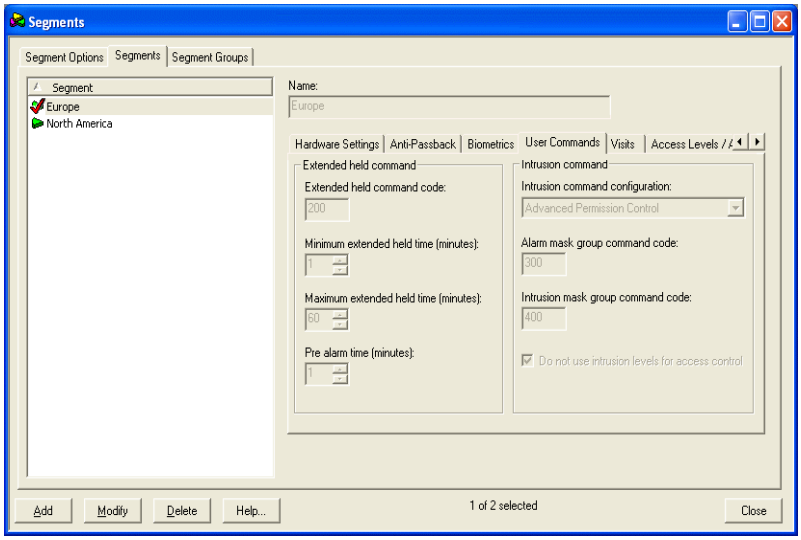
   c. Select the **Store minimum score per template** check box if you want minimum acceptance scores stored on a per template basis. If this check box is selected and the given template has a minimum acceptance score, the default will be overridden. If not selected, the default will be used. You assign minimum acceptance scores to templates in Multimedia Capture.
5. If you are working with Bioscrypt:
   a. Enter the maximum number of templates to be downloaded to the controller.
   b. Select the default security level which identifies the level of accuracy acceptable for template verification. Refer to the following table for rejection and acceptance rates per security level.

Security Level	False Rejection Rate	False Acceptance Rate
Very Low Security	1/10,000	1/100
Low Security	1/5,000	1/200
Medium Security	1/1,000	1/1,000
High Security	1/200	1/5,000
Very High Security	1/100	1/20,000

   c. Select the **Store security level per template** check box if you want to store individual security levels per template. Individual security levels are configured in Multimedia Capture. Leave this check box deselected if you want to use default security levels for all Bioscrypt templates.
      - If this check box is selected and the individual security level is set to “No Security”, then every Bioscrypt template will be successfully verified at the reader.
      - If this check box is not selected, then individual security levels are disabled, even though the security levels are still active in Multimedia Capture.
6. Click [OK].

Segments Form (User Command Sub-tab)

Note: This form displays when segmentation is enabled. When segmentation is not enabled, these options are available on the User Command form in the System Options folder.



Extended held command code

The held open time for some readers can be extended by a validated user at a command keypad. This field indicates the key sequence to use for the command. The command code key sequence must be between three and six digits. The default is 200.

Minimum extended held time (minutes)

Indicates the minimum number of minutes to extend the held open time to. The default is one.

Maximum extended held time (minutes)

Indicates the maximum number of minutes to extend the held open time to. The default is 60.

Pre alarm time (minutes)

Indicates the pre alarm time in minutes. This is the number of minutes before the held open time expires that a pre alarm will be generated. The default is one.

Intrusion command configuration

Select from the following intrusion command options:

- **Disabled** - The default setting disables use of the intrusion command code.
- **Global Permission Control Only - Allows use of the intrusion command code.** For more information please refer to Appendix J: Intrusion Command on page 1469.
- **Advanced Permission Control** - Allows the use of the intrusion command code and other advanced functionality used for Command Keypad Templates. For more information, refer to Chapter 34: Command Keypad Templates Folder on page 743.

Alarm mask group command code

If the **Global Permission Control Only** or **Advanced Permission Control** options are selected from the **Intrusion command configuration** drop-down then the Alarm mask group command code can be configured. The command code can be between 3 and 6 digits in length and can not match the command code that is used by the extended held command code or intrusion mask

group command code. For more information please refer to Appendix J: Intrusion Command on page 1469.

Intrusion mask group command code

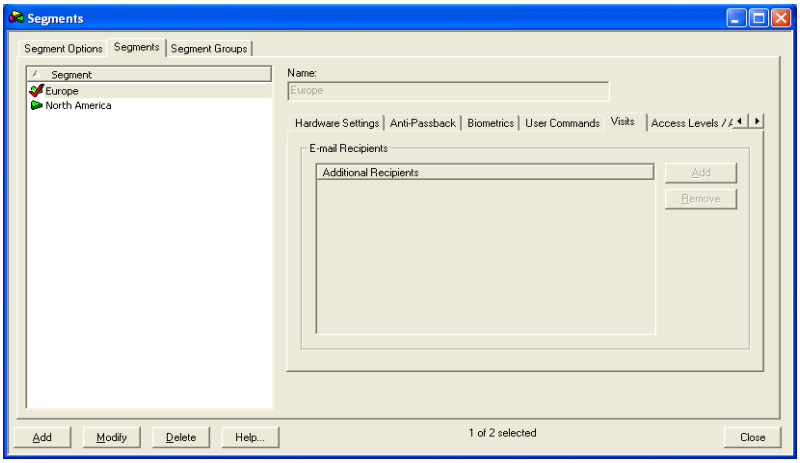
If the **Global Permission Control Only** or **Advanced Permission Control** options are selected from the **Intrusion command configuration** drop-down box then the Intrusion mask group command code can be configured. The command code can be between 3 and 6 digits in length and can not match the command code that is used by the extended held command code or alarm mask group command code. For more information please refer to Appendix J: Intrusion Command on page 1469.

Do not use intrusion levels for access control

Select to disallow cardholders automatic access control rights. To gain access control rights the cardholder must hold non-intrusion authority access levels. When this field is selected, intrusion authority levels assigned to a badge only allow control over executions of intrusion commands at the command keypad. Setting this option requires a database download to all access panels configured to be online.

Segments Form (Visits Sub-tab)

Note: This form displays when segmentation is enabled. When segmentation is not enabled, these options are available on the Visits form in the System Options folder.



Additional Recipients listing window

The recipients listed are the default recipients who will be e-mailed if the **Default Recipients** check box is selected on the E-mail form in the Visits folder.

Add

In modify mode, click this button to open the Add recipient window, from where you can locate a recipient. For more information, refer to Chapter 5: Visits Folder on page 145.

Remove

In modify mode, click this button to remove the selected recipient from the Additional Recipients listing window.

Modify
Changes the system options. When clicked, options on any form in the System Options folder can be modified.

Help
Displays online help for this topic.

Close
Closes the System Options folder.

Visits Sub-tab Procedures

The following procedures can be performed on this tab.

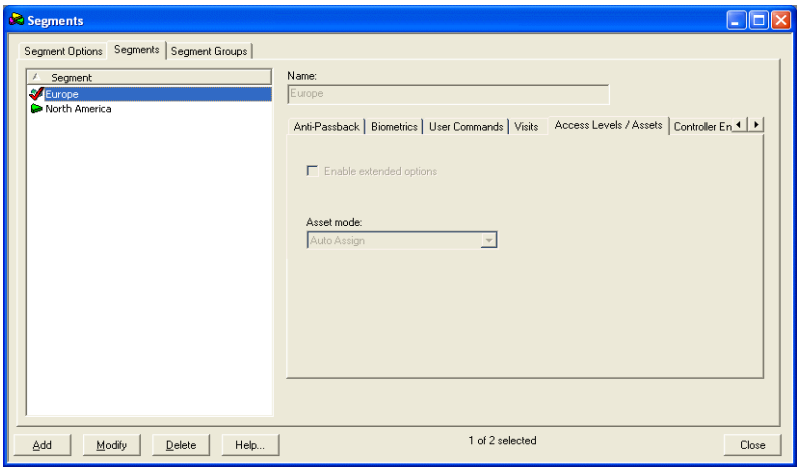
Configure Default E-mail Recipients (Segmented System)

The recipients listed in the Additional Recipients listing window for a selected segment are the default recipients who will be e-mailed if the **Default Recipients** check box is selected on the E-mail form in the Visits folder. To configure the default e-mail recipients:

1. On a segmented system, select the ***Administration*** > ***Segments*** menu option, click the Segments tab, and then click the Visits sub-tab. On a non-segmented system, select ***Administration*** > ***System Options***, then click the Visits tab.
2. On a segmented system, select a segment, then click [Modify]. On a non-segmented system, just click [Modify].
3. Click [Add].
4. The Add recipient window opens. You may add a cardholder, visitor, directory account, or SMTP address.
   - If you select the Cardholder radio button and click [OK], the Select Host Wizard: Search form opens. For more information, refer to Select Host Wizard: Search Form on page 168.
   - If you select the Visitor radio button and click [OK], the Select Visitor Wizard: Search form opens. For more information, refer to Select Visitor Wizard: Search Form on page 171.
   - If you select the Directory account radio button and click [OK], the Select Account window opens.
   - If you select the SMTP address radio button, type the SMTP address, then click [OK]. An example of an SMTP address is “joesmith@company.com”.
5. Click [OK].

Segments Form (Access Levels/Assets Sub-tab)

Note: This sub-tab displays when segmentation is enabled. When segmentation is not enabled, these options are available on the Access Levels/Asset form in the System Options folder.



Enable extended options

Select this check box to add escort functionality to access levels and enable the Access Levels/Assets folder >Extended Options form. Extending options requires additional memory and a full access panel download. Users on other workstations must log out/on in order to use the new settings. The **Enable extended options** check box should not be selected if asset management is going to be used.

Asset mode

Choose the asset mode you wish to choose. Options include:

- Tracking - assets will be assigned to a specific individual (In Alarm Monitoring, an Asset Privilege Only message will always be generated.)
- Auto Assign - assets will be assigned based on Groups and Classes. A cardholder can belong to one Group. A Group contains Classes. Assets also contain Classes. When Auto Assign is selected, if the Assets Class matches the Group Class, then permission to have the asset is granted.

To disable asset operations, set the Assets field on the LNL-2000 or LNL-1000 form in the Access Panels folder to 0.

It is advisable to determine and configure this option prior to entering any data into your system.

Enable Extended Options for Access Levels/Asset

The following procedure applies to segmented systems only. For non-segmented systems, refer to the System Options folder on the Access Levels/Assets form.

1. From the ***Administration*** menu, select ***Segments***, or click the Segments toolbar button.
2. Click the Segments tab. Click the Access Levels/Asset sub-tab.
3. Click [Modify].
4. Select the **Enable extended options** check box.

Note: To configure extend options for Access Levels (escort mode and activation times), refer to the Access Levels/Asset folder > Extended Options form. For more information, refer to Extended Options Form on page 729.

Segments Form (Controller Encryption Sub-tab)

The Controller Encryption form is used to:

- Configure the segment for encryption (automatic or manual)
- Enter master keys for encryption
- Export master keys to a text file
- Activate inactive keys (manual encryption only)

For more information regarding encryption, refer to the Encryption for Controllers User Guide.

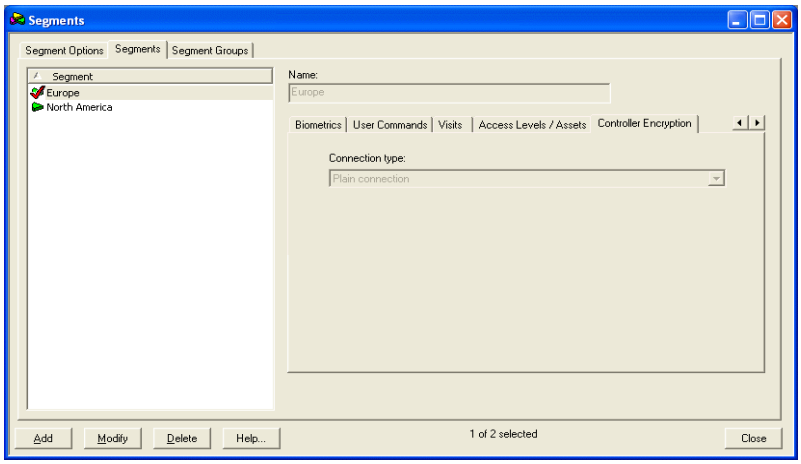
Note: This sub-tab displays when segmentation is enabled. When segmentation is not enabled, these options are available on the Controller Encryption form in the System Options folder.

To display the Controller Encryption sub-tab, select ***Segments*** from the ***Administration*** menu and click the Segments tab. Then, click the Controller Encryption sub-tab.

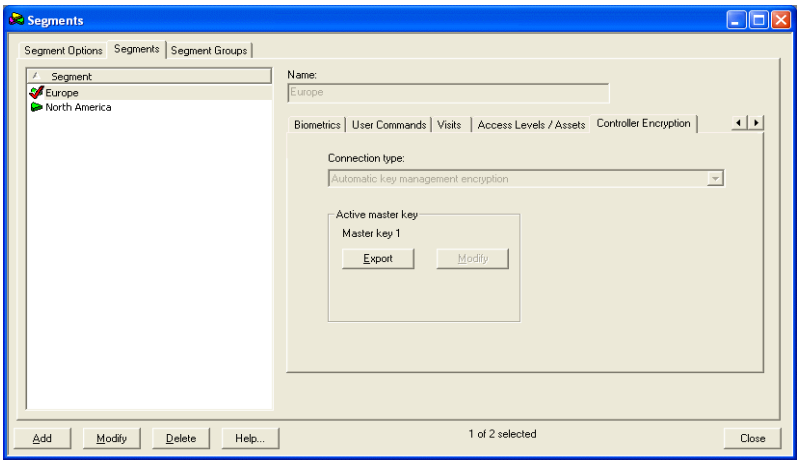
The Controller Encryption sub-tab is used to configure encryption for a system. This applies to Lenel controllers, Fire panels (ESPA, Notifier AM2020/NFS-640, Pyrotronics), Intercom Devices, Personal Safety Devices (Visonic Spider Alert), Receivers (Bosch 6500, SIA), Intrusion Panels (all except generic Intrusion), and POS Devices (TVC-2100 series). For more information, refer to the Access Panels Folder chapter.

The Controller Encryption form displays different fields depending on the connection type.

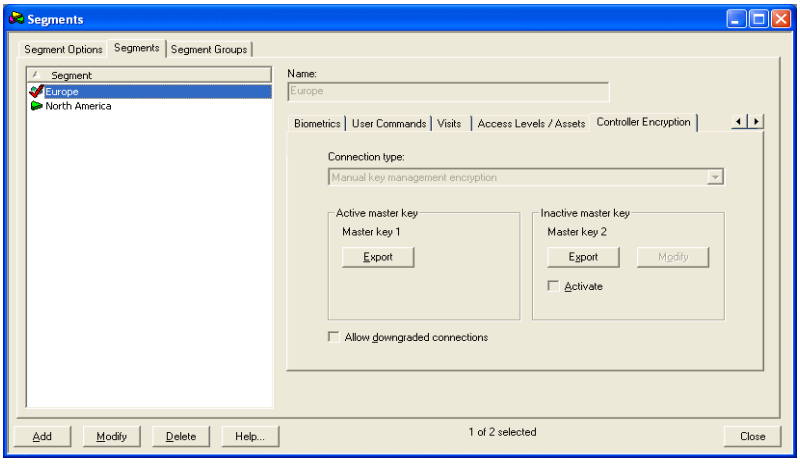
Plain Connection



Automatic Key Management Encryption



Manual Key Management Encryption



Connection type

The type of connection that exists between the controller and the host application. The default value is a plain connection.

Active master key

Displays the name of the active key, an export button and depending on the connection type, a modify button. If the connection type is automatic, the modify button displays. If the connection type is manual, the modify button does not display.

Active master key - Export

Exports the active master key to a text file. Depending on the status of your system, this may be master key one or two.

Active master key - Modify

Opens the Master Key Entry window where you can modify the active master key (one or two).

Note that you cannot modify the active master key using manual key management encryption; doing so would cause communication errors.

Inactive master key

Displays to the right of the Active master key section, regardless of which key is in/active. The inactive master key section includes the name of the inactive key, export and modify buttons, and the **Activate** check box. Displays only for manual key management segments.

Inactive master key - Export

Exports the inactive master key to a text file. Depending on the status of your segment, this may be master key one or two. Displays only for manual key management segments.

Inactive master key - Modify

Opens the Master Key Entry window where you can modify the inactive master key. Depending on the status of your system, this may be master key one or two. Displays only for manual key management segments.

Activate

Select this check box when you want OnGuard to begin using this key. Displays only in the inactive master key section for manual key management systems. You should not activate a master key until both the controller and OnGuard have the same value for the inactive key.

If using an encrypted connection to one of the supported panels (Fire, Intercom, Personal Safety, Receiver, Intrusion or POS Devices) do not activate a master key until both the encrypted communication device and OnGuard have the same value for the inactive key

Allow downgraded connections

Select this check box if you want the host/controller connection to downgrade the connection if the encryption connection fails. Displays only for manual key management segments.

Downgraded Connections

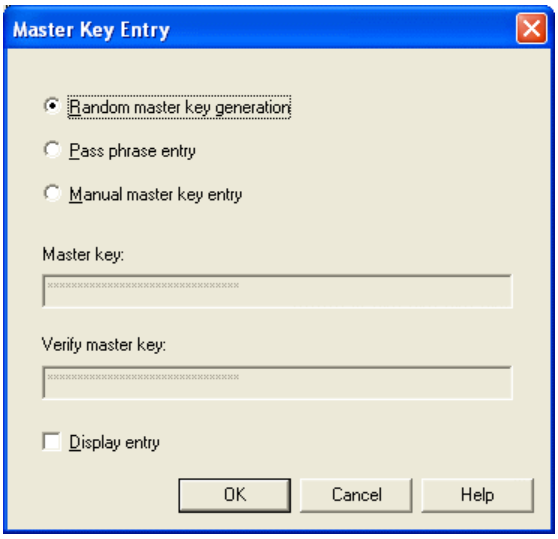
When this check box is selected, the access control system attempts the following connections (in sequence):

1. An encrypted connection with the inactive master key
2. An encrypted connection with the factory default value for Master Key 1
3. An encrypted connection with the factory default value for Master Key 2
4. A plain connection (only attempted if the controller does not require an encrypted connection)

If encryption is enabled the following connections are attempted in sequence:

1. An encrypted connection with the inactive master key.
2. A plain connection.

Master Key Entry Window



Random master key generation
Randomly generates a 128-bit value master key.

Pass phrase entry
Identifies the master key value as a pass phrase or sentence. The recommended minimum length for a pass phrase is 50 characters. The range of acceptable character length is between 1 and 255 characters. Spaces and symbols can be used and the pass phrase is case-sensitive. Notice when this radio button is selected, the text fields on this form change to Pass phrase and Verify pass phrase.

Manual master key entry
Identifies the master key value as a 128-bit value in hexadecimal form. A 128-bit hexadecimal value is exactly 32 digits containing any of the following numbers or letters: 0 – 9, A – F.

Master key/Pass phrase
The master key or pass phrase value.

Verify master key/Verify pass phrase
The master key or pass phrase value. This field verifies that you correctly entered the master key/pass phrase value. You cannot copy/paste between this field and the master key/pass phrase field.

Display entry
Displays the characters in the master/pass phrase fields if this check box is selected.

OK
Accepts the changes and closes the Master Key Entry window.

Cancel
Closes the Master Key Entry window.

Controller Encryption Sub-tab Procedures

The following procedures can be performed on this tab.

Configure Automatic Encryption and Set Keys

The encryption modify/export permission is required to complete this procedure.

1. Select ***Segments*** from the ***Administration*** menu, or click the Segments toolbar button.
2. Click the Segments tab. Click the Controller Encryption sub-tab.
3. Click [Modify].
4. If you are initially setting up automatic encryption:

Note: When encryption is being used with an encrypted communication device, the encryption key must be configured properly within the communication device first. The master key should then be configured on the Controller Encryption sub-tab. For more information, refer to Segments Form (Controller Encryption Sub-tab) on page 473.

   a. Select “Automatic key management encryption” from the **Connection type** drop-down list.
   b. Acknowledge any messages that display.
   c. Skip to step 6.
5. If you are updating the master key, click [Modify] (located in the active master key section of the sub-tab).
6. The Master Key Entry window opens. Select the **Manual master key entry, Pass phrase entry**, or **Random master key generation** radio button.
   - If you selected the **Manual master key entry** or **Pass phrase entry** radio button:
     i. Select the **Display entry** check box if you want to see the characters you are typing.
     ii. Enter and verify the master key/phrase. If the key is stored in a text file, you can copy/paste the key into these fields.
     iii. Click [OK].
     iv. Acknowledge any messages that display.
   - If you selected the **Random master key generation** radio button:
     i. Select the **Display entry** check box if you want to see the master key values.
     ii. Click [OK].
7. On the Controller Encryption form, click [OK].
8. Acknowledge any messages that display.

Configure Manual Encryption and Set Keys

When you initially configure manual encryption, you should modify both master keys to prevent a key with a factory default value from being used (security risk).

If encryption is being used for Lenel access control panels, then when you manually update a master key, you modify the inactive key and use the Lenel Controller Encryption Configuration Utility to load the new key into the controller. Once both the controller and OnGuard have the same value for the inactive key, you can activate the new key. For more information, refer to the Encryption for Controllers User Guide or the Lenel Controller Encryption Configuration Utility.

Note: When encryption is being used with an encrypted communication device, the encryption key must be configured properly within the communication device first. Then the

master key should be updated on the Controller Encryption form. Once the communication device and OnGuard have the same value for the inactive key, you can activate the new key.

The encryption modify/export permission is required to complete this procedure.

1. Select ***Segments*** from the ***Administration*** menu, or click the Segments toolbar button.
2. Click the Segments tab. Click the Controller Encryption sub-tab.
3. Click [Modify].
4. If you are updating a key, skip to step 5. If you are initially setting up manual encryption complete the following:
   a. Select “Manual key management encryption” from the **Connection type** drop-down list.
   b. Acknowledge any messages that display.
   c. Skip to step 6.
5. If you are updating a key, click [Modify] (located in the inactive master key section of the form).
6. The Master Key Entry window opens. Select the **Manual master key entry, Pass phrase entry**, or **Random master key generation** radio button.
   - If you selected the **Manual master key entry** or **Pass phrase entry** radio button:
     1) Select the **Display entry** check box if you want to see the characters you are typing.
     2) Enter and verify the master key/phrase. If the key is stored in a text file, you can copy/paste the key into these fields.
     3) Click [OK].
     4) Acknowledge any messages that display.
   - If you selected the **Random master key generation** radio button:
     1) Select the **Display entry** check box if you want to see the master key values.
     2) Click [OK].
7. On the Segments form, click [OK].
8. Acknowledge any messages that display.
9. If manual encryption is enabled for the first time, it is recommended that you update both master keys by repeating this procedure.

Modify Master Keys

If you want to automatically update/change keys, refer to Configure Automatic Encryption and Set Keys on page 477.

If you want to manually update/change keys, refer to Configure Manual Encryption and Set Keys on page 477.

Export Master Keys

This procedure applies to manual and automatic key management encryption systems. To export master keys:

1. Select ***Segments*** from the ***Administration*** menu, or click the Segments toolbar button.
2. Click the Segments tab. Click the Controller Encryption sub-tab.
3. Click [Export].
4. The Save As dialog opens. Enter the file name and click [Save].
5. Acknowledge any messages that display.

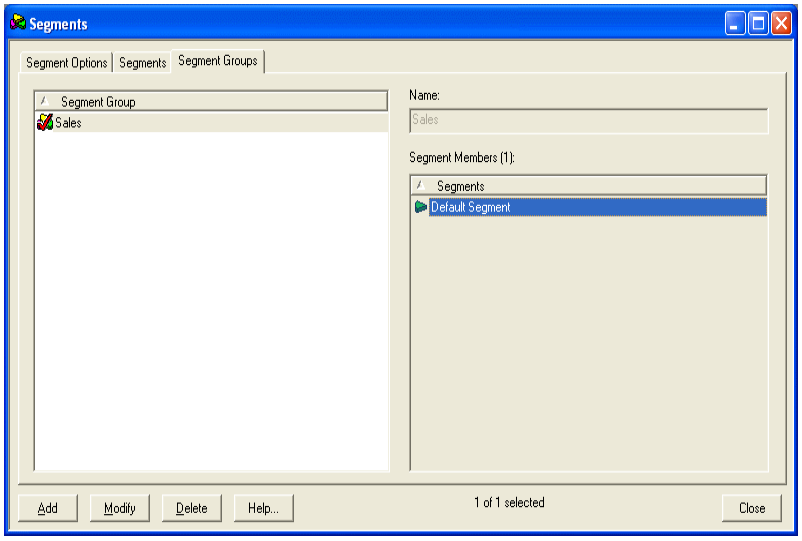
Activate Master Keys

The modify/export permission is required to complete this procedure.

1. Select ***Segments*** from the ***Administration*** menu, or click the Segments toolbar button.
2. Click the Segments tab. Click the Controller Encryption sub-tab.
3. Click [Modify].
4. Select the **Activate** check box.
5. Select the **Allow downgraded connections** check box if you want the host to controller connection to downgrade to a plain connection when the encryption connection fails.
6. Click [OK].
7. Acknowledge any messages that display.

Segment Groups Form

The Segment Groups form is used to add segment groups to your installation. This form is displayed only if you have enabled segmentation. For more information, refer to Configure an Installation to Use Segmentation on page 462. You must also have the appropriate permission group to view this form. Permission groups are set on the forms in the Users folder.



Segment Group listing window

Lists the names of all currently defined Segment Groups.

Name

Type a unique, descriptive name for the Segment Group.

Segment Members listing window

In “Add” and “Modify” mode, lists the names of all currently defined segments that are available to be included in a Segment Group. In “View” mode, lists the names of all segments included in the Segment Group that is currently selected in the Segment Group listing window.

Add

Adds a new segment group.

Modify
Changes an existing segment group.

Delete
Deletes an existing segment group.

Mode
In view mode, indicates the record/selection count (such as “1 of 42”). In modify mode, indicates the current operation, such as “Modify Mode.”

Help
Displays online help for this form.

Close
Closes the Segments folder

CHAPTER 19

List Builder Folder

The List Builder folder contains a form with which you can add, change, and delete the contents of lists that are used on the Cardholder form.

If you are using a segmented system you can add entries to the list builder which will then be filtered by the user's segments as well as any selected cardholder segments (if cardholder segmentation is enabled)

The folder contains one form, the Simple Lists form.

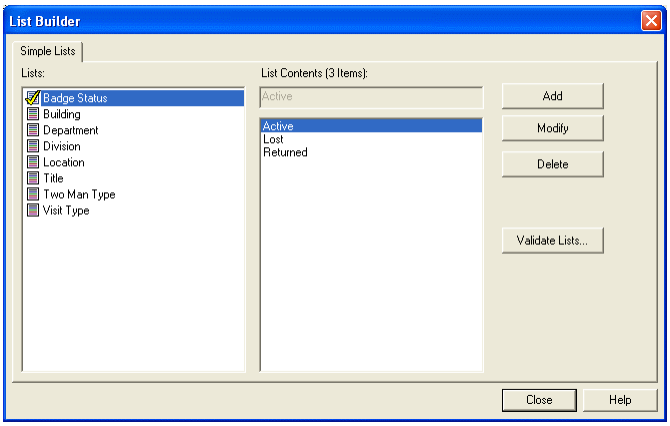
The List Builder folder is displayed by selecting ***List Builder*** from the ***Administration*** menu, or by selecting the List Builder toolbar button.

Toolbar Shortcut

Simple Lists Form

The Simple Lists form is used to add, change, and delete the contents of lists that are used throughout the software.

Note: The Two Man Type list cannot have its default list items deleted or modified. For more information, refer to Configure the List Builder for Special Two-Man Rule on page 1441.



Lists

Each entry is the name of a system-wide list whose contents can be changed. Some lists are common to all OnGuard installations; others are customer-specific.

List Contents (__ items)

Contains the edit window and the listing window.

edit window

For the selected list, displays the entry that is being added, changed, or deleted.

Listing window

Displays the current contents of the selected list

Add

Used to add an entry to the selected list.

Modify

Used to change an entry in the selected list.

Delete

Used to remove an entry from the selected list.

Validate Lists

Clicking this button causes the application to validate all list tables and cardholder records to ensure they contain valid values. This can be useful after performing data imports or adding/updating cardholder data using other database tools. If you encounter an error printing a badge that indicates the cardholder may be missing data for a field, using this button may fix the problem.

Close

Closes the List Builder folder.

Help

Displays online assistance for this form.

Simple Lists Form Procedures

Use the following procedures on this form.

Add an Entry to a List

Note: List Builder entries can also be added at child Enterprise servers. List Builder entries replicate as part of the Upload and Download available in Replicator, not part of System Table Download. List Builder entry transactions can be viewed in the Enterprise Transaction screen in Replication Administration. System List Builder lists are not editable on child regions (Badge Status, Two Man Type) they must be added at the Master and pushed via System Table Download in Replicator.

1. In the Lists section, select the name of the list. The contents of the list will be displayed in the listing window.
2. Click [Add].
3. If you have a segmented system you will be prompted to choose which segment you are adding the entry to.
4. In the edit window, type the item to add to the list.
5. Click [OK], or press the <Enter> key on your keyboard. The new item will be inserted alphabetically into the listing window.
6. Repeat steps 2 through 5 for each item to be added to the same list.

Modify an Entry in a List

1. In the Lists section, select the name of the list. The contents of the list will be displayed in the listing window.
2. In the listing window, select the entry you wish to change.
3. Click [Modify]. The entry will be displayed in the edit window.
4. In the edit window, make the change you want to the item.
5. Click [OK], or press the <Enter> key on your keyboard. The item will be revised in the listing window.

Delete an Entry from a List

1. In the Lists section, select the name of the list. The contents of the list will be displayed in the listing window.
2. In the listing window, select the entry you wish to delete.
3. Click [Delete]. The entry will be displayed in the edit window.
4. Click [OK] button, or press the <Enter> key on your keyboard.
5. Click [Yes] to confirm the deletion. The item will be removed from the listing window.

CHAPTER 20

MobileVerify Folder

The MobileVerify folder contains forms with which you can:

- Configure the system's current force protection setting.
- Configure gates.

The MobileVerify folder contains the System Settings form, and the Gates form.

This folder is displayed by selecting ***MobileVerify*** from the ***Administration*** menu.

MobileVerify Overview

MobileVerify is a software application specifically designed for OnGuard Enterprise solutions. MobileVerify enables a security officer, guard, or sentry to use an optional scanner or reader and automatically search the database for access privileges. The officer is instantly presented with the system's access granted or access denied recommendation. The process can be performed in either standalone or online mode.

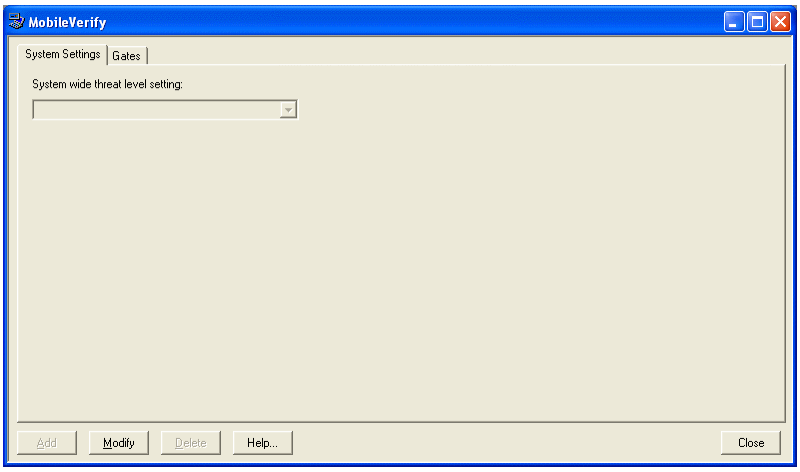
A wearable computer handles all of the client functions, and connects to the OnGuard server via 802.11b wireless Ethernet standards. The computer that has Mobile Enterprise installed on it has a PCMCIA slot for insertion of a wireless network card. The wireless network is designed, acquired and attenuated, providing connectivity between the Mobile Enterprise computer and the wireless access (connectivity) point on the secure side of the network. Without a network connection, Mobile Enterprise can be reconfigured to operate in a standalone mode.

Before configuring the system's current force protection setting and gates:

- Readers must be configured.
- FormsDesigner must be configured for MobileVerify.
- A Force Protection Setting list must be created and populated in the List Builder folder.

Refer to the MobileVerify User Guide for detailed configuration information.

System Settings Form



System wide threat level setting

Select your system's current force protection setting. Force protection settings are configured in the List Builder folder. For more information on force protection settings and MobileVerify, refer to the MobileVerify User Guide.

By default, the name of this field is **System wide threat level setting**. However, the name may change depending on your configurations in FormsDesigner. For more information, refer to the FormsDesigner Configuration chapter in the MobileVerify User Guide.

Modify

Click this button to change the system wide force protection setting.

Help

Click this button to display online help for this form.

Close

Click this button to close the MobileVerify folder.

System Settings Form Procedures

Use the following procedures on this form.

Configure the System's Force Protection Setting

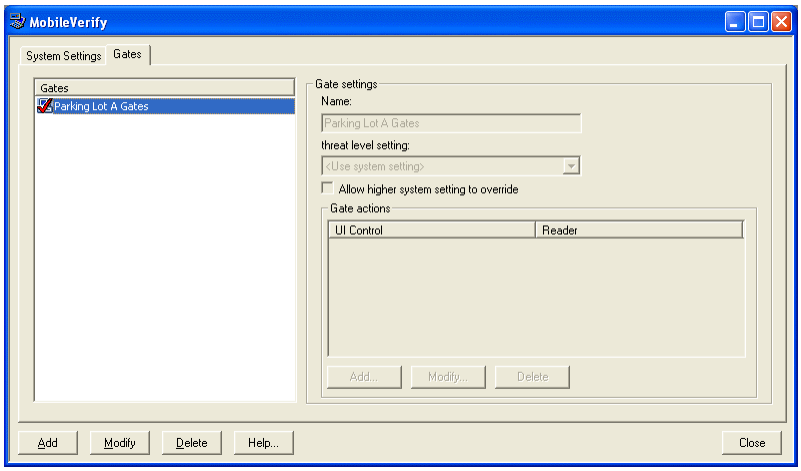
1. From the ***Administration*** menu, select ***MobileVerify***. The MobileVerify folder opens.
2. Click [Modify].
3. Select a force protection setting from the **System wide threat level setting** drop-down list.

   If your force protection settings are named "1) Normal," "2) Alpha," "3) Bravo," "4) Charlie," and "5) Delta," "5) Delta" is the highest force protection setting, and "1) Normal" is the lowest. If your force protection settings are named "1) DEFCON 5," "2) DEFCON 4," "3) DEFCON 3," "4) DEFCON 2" and "5) DEFCON 1," "1) DEFCON 5" is the lowest force protection setting and "5) DEFCON 1" is the highest. Force protection settings are defined in the List Builder folder. For more information, refer to the MobileVerify User Guide.

By default, the name of this field is **System wide threat level setting**. However, the name may change depending on your configurations in FormsDesigner. For more information, refer to the FormsDesigner Configuration chapter in the MobileVerify User Guide.

4. Click [OK].

Gates Form



Gates listing window

Displays a list of all gates that have been configured in the system.

Name

Specifies the name of the gate./

threat level setting

Specifies the selected gate's force protection setting. Force protection settings are configured in the List Builder folder. For more information on force protection settings and MobileVerify, refer to the MobileVerify User Guide.

When the <Use system setting> choice is selected, the system will use the setting selected in the **System wide threat level** field on the System Settings form in this folder.

By default, the name of this field is **threat level setting**. However, the name may change depending on your configurations in FormsDesigner. For more information, refer to the FormsDesigner Configuration chapter in the MobileVerify User Guide.

Allow higher system setting to override

If this check box is selected, a higher system wide force protection setting (configured on the System Settings form) will override the selected gate's force protection setting (configured on this form).

UI Control/Reader listing window

Displays the current UI control/reader configurations.

Add

In the Gate actions section, click this button to display the Select UI Control/Reader window from where you can configure the UI control for a grant or deny recommendation.

Modify
In the Gate actions section, click this button to display the Select UI Control/Reader window so that you can modify an existing UI control/reader configuration.

Delete
In the Gate actions section, click this button to display the Select UI Control/Reader window so that you can delete an existing UI control/reader configuration.

Add
Click this button to enter add mode from where you can add a gate.

Modify
Click this button to enter modify mode from where you can modify existing gate configurations.

Delete
Click this button to delete the gate selected in the Gates listing window.

Help
Click this button to display online help for this form.

Close
Click this button to close the MobileVerify folder.

Gates Form Procedures

Use the following procedures on this form.

Configure Gates

1. From the ***Administration*** menu, select ***MobileVerify***. The MobileVerify folder opens.
2. Select the Gates tab.
3. Click [Add].
4. In the Name field, type in the name of the gate. For example: `Parking lot A gate`.
5. From the **threat level setting** drop-down list, select this gate's force protection setting.

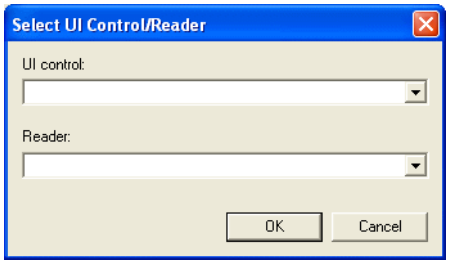
Notes: Force protection settings are configured in the List Builder folder. For more information on force protection settings and MobileVerify, refer to the MobileVerify User Guide.

When the <Use system setting> choice is selected, the system will use the setting selected in the **System wide threat level** field on the System Settings form in this folder.

By default, the name of this field is **threat level setting**. However, the name may change depending on your configurations in FormsDesigner. For more information, refer to the FormsDesigner Configuration chapter in the MobileVerify User Guide.

6. Select the **Allow higher system setting to override** check box if you want higher system wide force protection settings (configured on the System Settings form) to override the gate's force protection setting.
7. To configure the UI control for a grant (for example, when a guard receives a grant recommendation and selects the grant button, a specific door opens):

a. Click [Add]. The Select UI Control/Reader window is displayed.



b. From the **UI control** drop-down list, select “Grant Access.”

Note: The drop-down list options depend on what you named your recommendation buttons in FormsDesigner. For more information, refer to the MobileVerify User Guide.

c. From the **Reader** drop-down list, select the name of the reader that corresponds to this gate.

d. Click [OK].

8. To configure the UI control for a deny, repeat step 7. However, this time make sure to select “Deny Access” (or whatever your recommendation button is named), in the **UI control** drop-down list.

9. On the Gates form, click [OK].

CHAPTER 21

DataConduIT Message Queues Folder

The DataConduIT Message Queues folder contains forms with which you can:

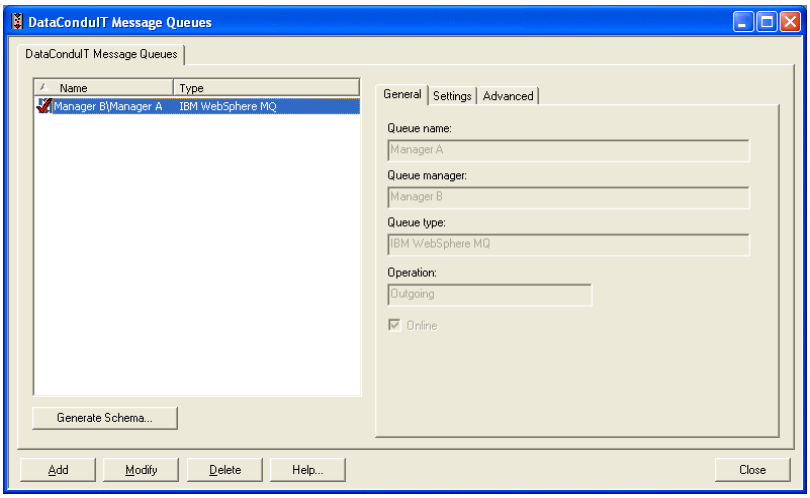
- Add, modify, or delete DataConduIT message queues.
- Generate a schema for the user to reference.
- Configure whether photo and signature information is included in messages.
- Configure when messages are sent.
- Add, modify, or delete a custom object event WMI query, custom access and security event WMI query.

The DataConduIT Message Queues folder contains one form: the DataConduIT Message Queues form. The DataConduIT Message Queues form contains three sub-tabs: General, Settings, and Advanced.

This folder is displayed by selecting ***DataConduIT Message Queues*** from the ***Administration*** menu.

For more information about DataConduIT Message Queues, refer to the DataConduIT User Guide.

DataConduIT Message Queues Form (General Sub-tab)



Listing window

Lists currently defined DataConduIT message queues. Each entry contains the queue's name and type.

Generate Schema

Generates a schema for you to reference. If clicked, the Save As window is displayed, and you must select where to save the schema.

After any changes to the database have been made using FormsDesigner, you must regenerate the schema so that the updated database is reflected in the schema file.

DataConduIT uses the Windows account of the person who is logged on to the machine at the time of schema creation. Because of this, it is probably more preferable for a system administrator to handle all schema generation.

Add

Click this button to add a DataConduIT message queue.

Modify

Click this button to change a selected DataConduIT message queue.

Delete

Click this button to delete a selected DataConduIT message queue.

Help

Displays online help for this form.

Close

Closes the DataConduIT Message Queues folder.

Queue name

Enter the queue's name. This field is case-sensitive.

Queue/SNMP manager

This field does not pertain to Microsoft Message Queues. If adding an IBM WebSphere MQ queue, enter the queue manager's name. This field is case-sensitive. If adding an SNMP Trap

Messages queue, enter the SNMP manager's IP address. Depending on the network configuration, a fully qualified NetBios name may be required.

Queue type

OnGuard supports the following types of queues: IBM WebSphere MQ, Microsoft Message Queue, and SNMP Trap Messages. The queue type is selected when a queue is added, and it cannot be modified after the queue has been added.

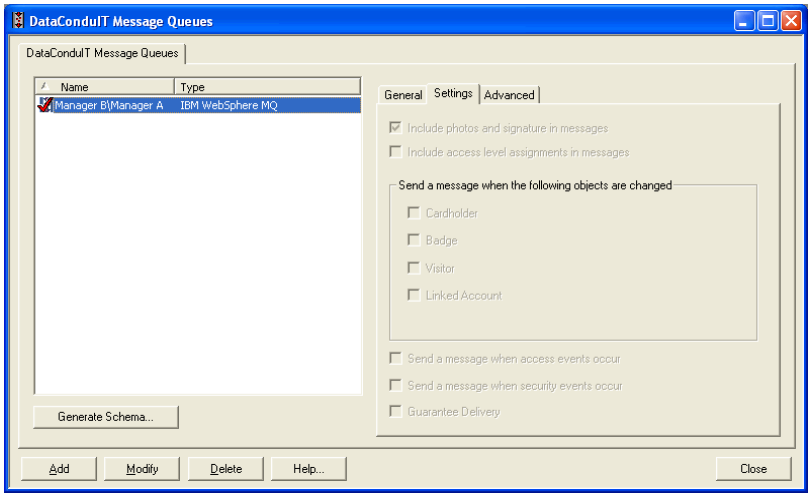
Operation

The IBM WebSphere MQ queue type supports two operations: incoming and outgoing. A queue is designated as either incoming or outgoing when it is added. The SNMP Trap Messages queue type only supports outgoing queues. The operation cannot be modified after a queue has been added.

Online

Shows whether the queue is online or offline. While checked the queue is online and will function normally. Unchecked makes the queue become offline. Being offline means no events are sent or received from the queue.

DataConduIT Message Queues Form (Settings Sub-tab)



Note: This sub-tab is only displayed for outgoing queues.

Include photos and signature in messages

Specifies whether photos, signatures, and fingerprints are included in messages. If this option is selected, the size of the messages sent is much larger.

Include access level assignments in messages

Check this box to include access level assignments in the outgoing messages.

Cardholder

If selected, a message will be sent whenever a cardholder record is added, modified, or deleted.

Badge

If selected, a message will be sent whenever a badge record is added, modified, or deleted.

Visitor
If selected, a message will be sent whenever a visitor record is added, modified, or deleted.

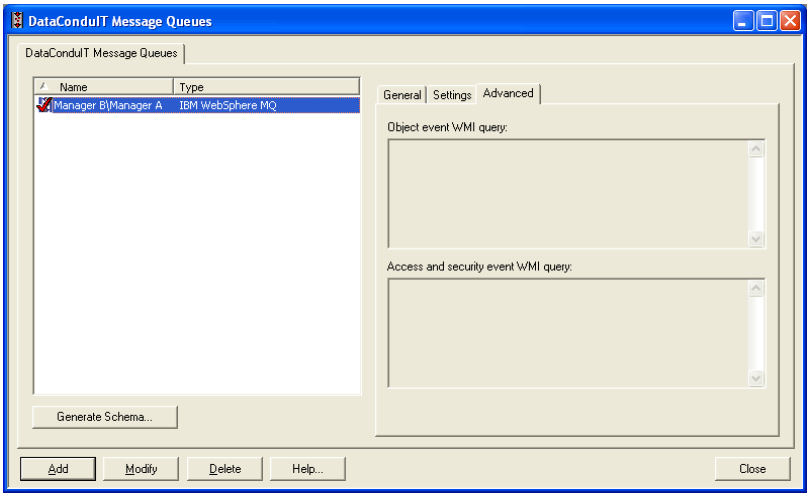
Linked Account
If selected, a message will be sent whenever a linked account record is added, modified, or deleted.

Send a message when access events occur
If selected, a message will be sent every time an access event occurs. Two examples of access events are access granted and access denied events.

Send a message when security events occur
If selected, a message will be sent every time a security event occurs. Two examples of security events are door forced open and alarm restored events.

Guarantee Delivery
Check this box to guarantee delivery of hardware events. This works by first sending the events to a table where the DataConduITQueue will then retrieve them. The guarantee is assured because the table is used as a preliminary queue and the events are not deleted until picked up by the DataConduITQueue. The DataConduITQueue will not mark the event as processed until it is written on the designated message queue. There is a mathematically small possibility that you could receive a duplicate event, but the chances are negligible.

DataConduIT Message Queues Form (Advanced Sub-tab)



Note: This sub-tab is only displayed for outgoing queues.

Object event WMI query
You can type an object event WMI query in directly. Objects include cardholders, linked accounts, badges, and visitors.

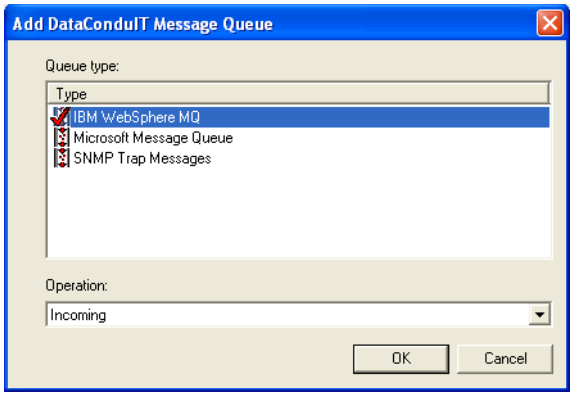
Access and security event WMI query
You can type an access and security event WMI query in directly. Access events are events such as access granted and access denied. Security events are events such as door forced open and alarm restored.

DataConduIT Message Queues Form Procedures

Use the following procedures on this form.

Add DataConduIT Message Queue

1. From the ***Administration*** menu, select ***DataConduIT Message Queues***.
2. On the DataConduIT Message Queues form, click the [Add] button.
3. The Add DataConduIT Message Queue window opens.
   a. Select the queue **Type**.
   b. Select the queue **Operation**. The operation cannot be modified after a queue has been added.
      - The Microsoft Message Queue and IBM WebSphere MQ queue types support two operations: incoming and outgoing.
      - The SNMP Trap Messages queue type supports only the outgoing operation.



   c. Click [OK].
4. On the General sub-tab:
   a. In the **Queue name** field, type the name of the queue. The name is case-sensitive. For IBM WebSphere MQ queues, this name must be exactly the same name that you used when setting up the queue in the IBM WebSphere MQ software.
   b. In the **Queue manager or SNMP manager** field, enter the manager's name. If adding an IBM WebSphere MQ queue, enter the queue manager's name. If adding an SNMP Trap Messages queue, enter the SNMP manager's IP address. Depending on the network configuration, a fully qualified NetBios name may be required. If adding a Microsoft Message Queue this field is not present.
   c. Note that the **Queue type** and **Operation** that you selected are displayed, but cannot be modified.
5. If you added an incoming queue, click [OK] and the queue will be added. If you added an outgoing queue, continue on to step 6.
6. On the Settings sub-tab:
   a. If you wish to have photo, signature, and fingerprint information sent in messages, select the **Include photos and signature in messages** check box.

Note: Including photo information in the messages makes the size of the message sent much larger.

b. Select whether a message will be sent when cardholder, badge, visitor, and linked accounts are added, modified, or deleted.

c. If you wish to have a message sent when an access event occurs, select the **Send a message when access events occur** check box.

d. If you wish to have a message sent when a security event occurs, select the **Send a message when security events** occur check box.

7. Using the Advanced sub-tab is optional and for advanced users. On the Advanced sub-tab you may:

   a. Type an object event WMI query directly into the **Object event WMI query** textbox.

   b. Type an access and security event WMI query directly into the **Access and security event WMI query** textbox.

8. Click the [OK] button.

Note: If you configured an SNMP Trap Messages queue, load the **lenel.mib** file into the SNMP Manager so that it knows how to handle and display the variables it receives. The Lenel MIB file is located in the **Support Center/SNMP** folder on the Supplemental Materials disc.

Modify a DataConduIT Message Queue

1. From the ***Administration*** menu, select ***DataConduIT Message Queues***.
2. In the listing window of the DataConduIT Message Queues form, select the queue record you wish to modify.
3. Click the [Modify] button.
4. Make the changes you want to the fields. Changes can be made on any sub-tab.
5. Click the [OK] button to save the changes, or the [Cancel] button to revert to the previously saved values.

Delete a DataConduIT Message Queue

1. From the ***Administration*** menu, select ***DataConduIT Message Queues***.
2. In the listing window of the DataConduIT Message Queues form, select the queue record you wish to delete.
3. Click the [Delete] button.
4. Click the [OK] button.
5. Click the [Yes] button to confirm the deletion.

CHAPTER 22

Text Library Folder

The Text Library folder contains a form with which you can create text entries that can be used as additional parameters for when they are linked to the alarm or global I/O input events.

Note: Currently the only components that support Text Library linking are Alarm Configuration and Global I/O.

The Text Library folder is displayed by selecting ***Text Library*** from the ***Administration*** menu.

Toolbar Shortcut

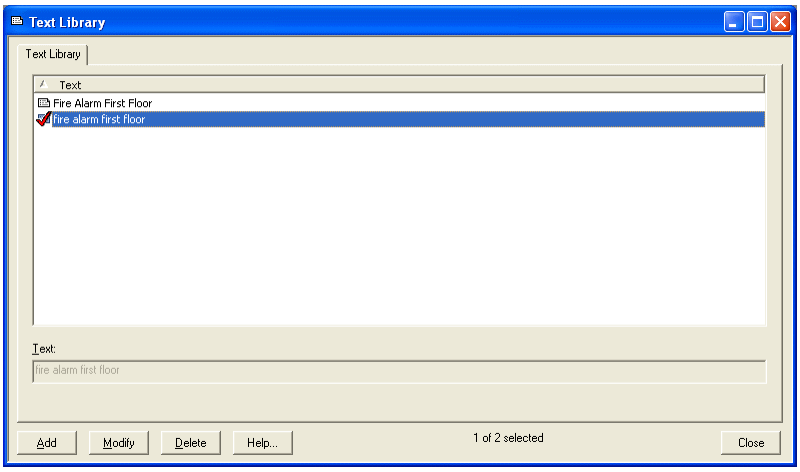
Adding your own custom text entries allows you to modify and work with generic events based on the event text you created for them in the text library. Through the text library, you create different text entries that are then used when modifying alarms for the generic event.

The Generic Event event conveys no information other than to indicate that an event has occurred. Once you modify the Generic Event event to run after a certain alarm is triggered you can create a text entry to match the action. For example you could create a Generic Event event for a fire alarm on the first floor of your building. You could then create a text entry “Fire alarm - First floor.”

When creating a Generic Event event you are presented with a drop-down list with your text entries. You select the “Fire alarm - First floor” and that becomes the Generic Events event text. Once that Generic Event is triggered the event text is matched to the text library. If a match is found, the alarm specified with that event text is shown in Alarm Monitoring.

Note: If you have the correct permissions you can add text directly to the **Event text** drop-down list when modifying a Generic Event. If the text you enter isn’t in the text library it will be added.

Text Library Form



Text
Lists the text entries that have already been entered by a user.

Text
Type the name of the Text Library entry. Once added, the name appears in the text display. The text library cannot contain any duplicate names and is limited to a maximum of 2000 characters per entry. text entries are also case-sensitive so you could have “Fire” and “fire” be separate text entries.

Add
Click this button to add a text entry.

Modify
Click this button to modify an existing text entry.

Delete
Click this button to delete an existing text entry.

Help
Displays online help for this form.

Close
Closes the Text Library folder.

Text Library Form Procedures

Use the following procedures on this form.

Add a Text Library Entry

1. From the ***Administration*** menu, select ***Text Library***.
2. On the Text Library form, click [Add].

3. In the **Text** text box, enter the name of the text entry, that you want to be available when linking to alarm or global I/O input events.
4. Click [OK].

The text entry is now displayed in the **Text** display area.

Modify a Text Library Entry

1. From the ***Administration*** menu, select ***Text Library***.
2. On the Text Library form, select the Text Library entry you want to modify.
3. Click [Modify].
4. Change the name of the text entry. Be aware that modifying the text entry also affects all the linked devices.

Delete a Text Library Entry

1. From the ***Administration*** menu, select ***Text Library***.
2. On the Text Library form, select the Text Library entry you want to delete.
3. Click [Delete].
4. Click [OK]. The text entry is now deleted.

Note: A text entry cannot be deleted if it is currently linked to other items. When you try to delete a linked entry you are presented with a list of linked items. You then have to unlink them before continuing.

Linking to the Text Library Entry

Once you have added a text library entry you can link it to either a Global I/O input event by using Add a Global I/O Linkage on page 814 or a custom alarm by using Add a Custom Alarm on page 856.

CHAPTER 23

Archives Folder

This folder allows you to archive Events, Events Video Location, Alarm Acknowledgments, User Transactions, Visits Records, and specific event types to text files in order to free up space in their respective database tables. This is an important task for the System Administrator to do on an ongoing basis, because allowing these records to build up can eventually fill up the allocated database space and adversely affect system performance.

The frequency and settings with which you archive will depend on what is appropriate for your security system and how long you must keep events and records online for reporting purposes. Archived records can always be restored to the database (provided you still have the archive files) and used for historical reporting.

The archive process is NOT an automated or scheduled process; you must manually run the archive process on an ongoing basis using the [Archive/Purge Now] button.

The Archives folder contains forms with which you can:

Archive:

- Indicate the frequency with which each type of record will be moved, and to where
- Preview record counts per every record type matching record archive configuration
- Move records from the database to a text file (called an *archive file*) located in the specified path
- Force immediate archival of video recordings that are associated with events but haven't been archived yet
- Purge events from the database
- Specify which event types should be archived

Restore:

- View a list of all archive files that have been created
- Restore Records from an archive file to the database
- Delete an archive file from the system
- Delete restored records from the database

The folder contains two forms: the Archiving form and the Restoring form.

The Archives folder is displayed by selecting ***Archives*** from the ***Administration*** menu or by selecting the Archives toolbar button.

Toolbar Shortcut

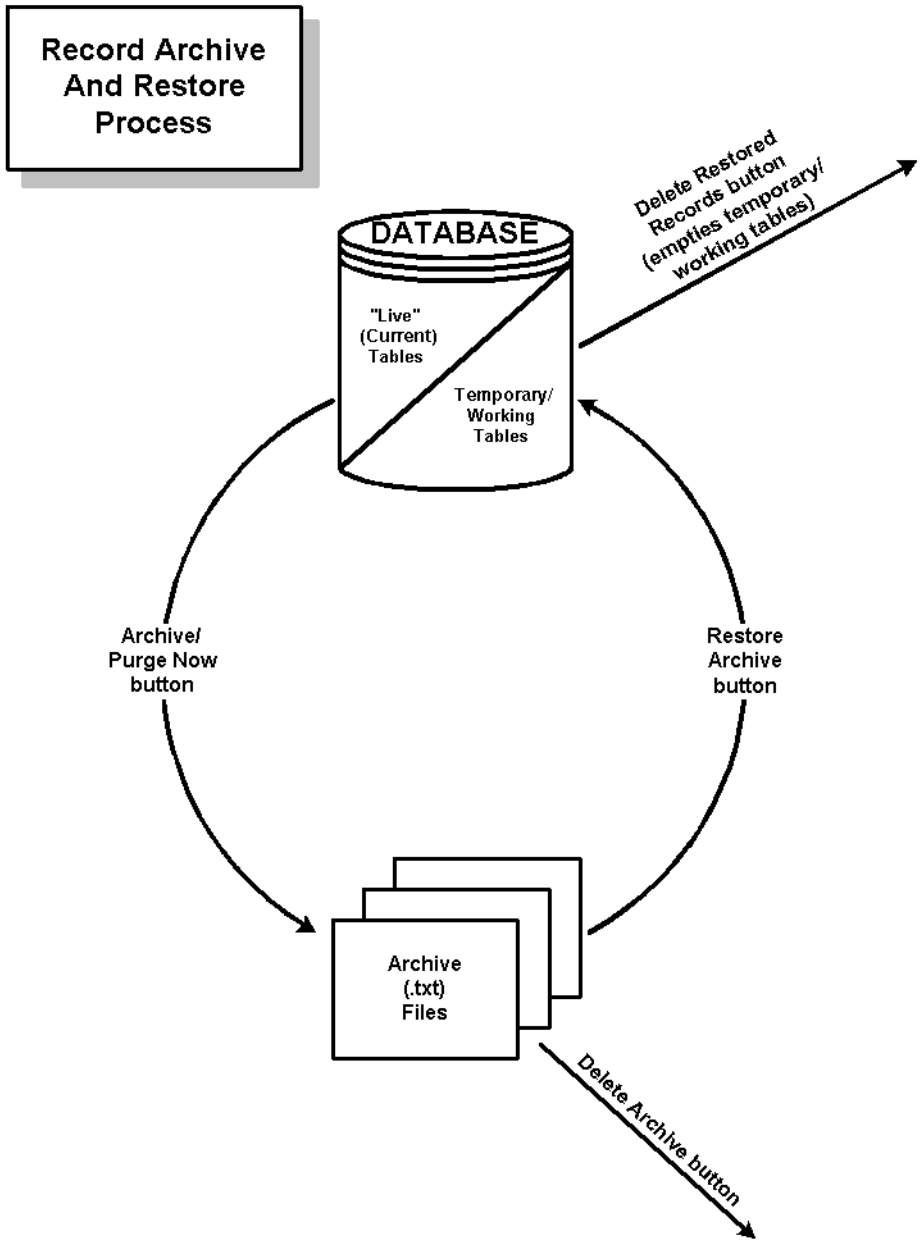
Visit Records

The criteria for archiving visit records is different from the criteria for archiving other types of records or events.

A visit that is currently signed in, regardless of the date, will not be archived. For archival to occur, the visit must be signed out.

Once signed out, the criteria for archiving the visit is based on the scheduled time out of the visit event. This ensures that visits scheduled in advance will not be archived before the actual visit occurs.

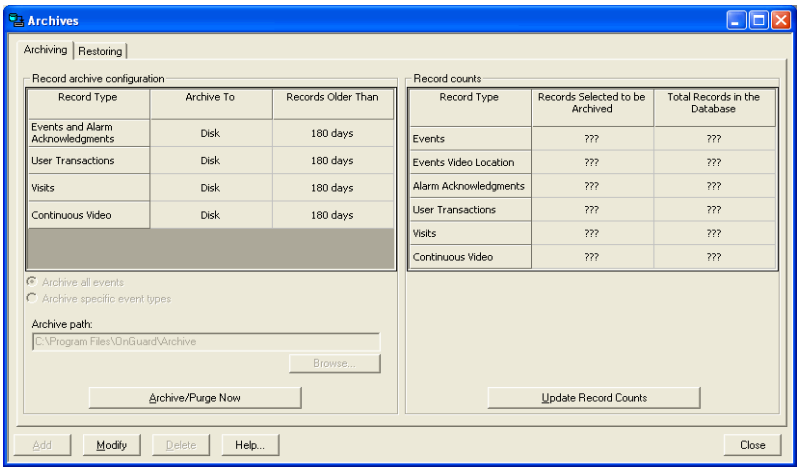
Record Archive & Restore Processes



Archiving Form

The Archives form is used to:

- Indicate the frequency with which each type of records will be archived, and to where.
- Archive - move records from the database to a text file (called an *archive file*) located in the specified path (Archive To: Disk).
- Purge - delete records from the system [Archive To: None (Delete Only)].



Record Archive Configuration

Includes Record Type, Archive To, Records Older Than, and Archive Path sections. In this section you can select whether or not they will archive all events or events belonging to a specific event type. Use this section to choose settings for many record types. These include: Access Denied, Access Granted, Area APB, Asset, Biometric, Burglary, C900, Duress, Fire, Gas, Generic, Intercom, Medical, Muster, Open/Close, Point of Sale, Relay/Sounder, System, Temperature, Transmitter, Trouble, Video, Water.

If the user does not have a license for receivers or intrusion panels the Trouble, Burglary, Temperature, Gas, Relay Sounder, Medical, Water, C900, and Open Close event types must not be listed in the event type archiving configuration or in the record counts section.

Archive To

For a particular **Record Type**, indicate what will be done with those Records that have been in the database longer than the **Records Older Than** value. Choose one of the following:

- Disk - the events/Records will be stored in a text file on the disk, in the directory specified by the **Archive Path** field. The name of the text file identifies the date the archive was performed and the **Record Type**.
- None (Delete only) - the records will be deleted from the system. This means, that they are then PERMANENTLY LOST.

To bulk change the entire column double click on the **Archive To** column and follow the dialog prompts.

Records Older Than

For a particular **Record Type**, indicate the number of days after which this type of Record will be archived. You can specify a number in the range of 1 through 3650 (which is approximately 10 years).

Access Denied, Access Granted, Area APB, Asset, Biometric, Burglary, C900, Duress, Fire, Gas, Generic, Intercom, Medical, Muster, Open/Close, Point of Sale, Relay/Sounder, System, Temperature, Transmitter, Trouble, Video, and Water are governed by the same **Records Older Than** setting to maintain data integrity.

To bulk change the entire column double click on the **Records Older Than** column and follow the dialog prompts.

If you have both an “Archive To” and “Records Older Then” item selected and you right-click, another dialog will be displayed allowing you to set both of these items.

Archive all events

If selected, the Record Archive Configuration listing window will show the basic record types to be archived and purged.

Archive specific event types

If selected, the Record Archive Configuration listing window will show a nested grid control to choose specific events that can be archived and purged. These will be shown in a nested tree under the Events and Alarm Acknowledgments Record Type.

Archive Path

Indicates the drive and directory where archive files will be stored. Type a path here, or click [Browse] to select one.

It is good practice to create one common shared directory on the network for archives, and to set this field to that path. That way, the same directory will be used no matter which workstation you archive from.

If you want to archive events for a specific event type and keep it isolated from a path that contains archives for all events as well, then you should specify a separate path.

Note that Universal Naming Convention (UNC) paths are supported (e.g., **\\Server_Name\C_Drive\Archives**).

Browse

Opens a Browse for Folder window, from which you can select a Archive Path.

Archive/Purge Now

Removes from the database all events/Records that meet the Records Older Than criteria specified for each Record Type. The removed events/Records are then handled in the manner specified in the Archive To section.

Record Counts

Includes Record Type, Records Selected to be Archived, and Total Records in the Database sections. Use this form to view the number of currently stored Records that meet the archive age (**Records Older Than**) criteria as well as the total number of records of particular **Record Type** currently stored in the database.

When the **Archive specific event types** option is selected, record counts will be updated to list out the specific event types that apply under Events, Alarm Acknowledgments, and Events Video Location. This is because these counts may differ for a specific event type for each of these three record types.

Records Selected to be Archived

For a particular **Record Type**, indicates the number of currently stored Records that meet the archive age (**Records Older Than**) criteria. It is the number of Records of each type that would be archived or purged if you were to click [Archive/Purge Now]. This information comes from the database; you cannot change it directly. To update the display, click [Update Record Counts].

Total Records in the Database

For a particular Record Type, indicates the total number of Records currently stored in the database. This information is generated from the database; you cannot change it directly. To update the display, click [Update Record Counts].

Update Record Counts

Polls the database and updates the count displayed in the **Records Selected to be Archived** and **Total Records in the Database** fields. The processing that occurs when selecting Update Record Counts could take a while if many events, user transactions, etc. are contained in the database.

When the **Archive specific event types** option is selected and you select **Update Record Counts**, the counts for the specific event types under Events, Alarm Acknowledgments and Events Video Location will only be calculated if the tree item has been expanded for these. If you do not need one or more of these counts, and wants to speed up the count processing, it is better to collapse these items.

Modify

Used to change Record Archive Configuration

OK

Used to accept changes to Record Archive Configuration (Modify Mode only)

Help

Displays pertinent help information on screen

Mode

(modify mode only) Indicates the current operation, such as “Modify Mode”

Close

Closes the Archives folder

Archiving Form Procedures

The following procedures can be performed on this form.

Configure Archive Parameters

1. With the **Archive all events** radio button selected, Click [Modify].
2. Working from left to right, row by row, select **Archive To** and **Records Older Than** values for each **Record Type**.
3. In the **Archive Path** field, type the drive and directory where you want archive files to be stored. Or, click [Browse] to navigate to the desired path, then click [OK] to insert the path into the field.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Archive Specific Event Types

Archiving and purging specific event types is useful when archiving all events create files that are too large and impossible to restore or the user only wants more flexibility regarding when events of a specific type will be archived. For example, the Granted and Denied event types may accumulate in the database faster than other event types, therefore the user may want to archive/purge these more often.

1. On the Archives folder click [Modify].
2. Select the **Archive specific event types** radio button. The Record archive configuration listing window switches to a nesting view.

3. In the Archive To column, select which events are to be archived to disk and which are to be deleted.
4. In the Records Older Than column, select the age of the event to be archived/purged.
5. In the **Archive Path** field, type the drive and directory where you want archive files to be stored. Or, click [Browse] to navigate to the desired path, then click [OK] to insert the path into the field.
6. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Archive Database Records

Note: You can perform this procedure only if the **Archive Transactions** check box is selected for your user account on the Software Options sub-tab of the System Levels form in the Users folder.

1. If you wish to know how many records of each type meet the specified elapsed time criteria, click [Update Record Counts]. This will update the numerical values in the Records Selected to be Archived and Total Records in the Database columns.
2. Select one of the following radio buttons:
   - **Archive all events**: Select this to archive and purge the events shown in the Record Archive Configuration listing window.
   - **Archive specific event types**: Select this to archive and purge the specific events shown in the Record Archive Configuration listing window. These will be shown in a nested tree under the Events Record Type.

Note: When performing the archive/purge operation, the user can not change the **Archive all events** or **Archive specific event types** options. This can only be done when in modify mode and is stored as part of the archiving configuration.

3. Click [Archive/Purge Now].
4. Click [Yes] to confirm the action.

   All records that have been in the database longer than their **Records Older Than** number of days will be archived. The transactions will be archived to disk or deleted, as specified in the **Archive To** field.

   If you wish to cancel the archival/purge of records, click [Cancel] that appears in the status dialog.

Note: Records will not be automatically archived, even if the database is getting full or if the Records Older Than value is exceeded. You must click [Archive/Purge Now] to actually initiate the archive process.

Data Integrity

In order to maintain data integrity Alarm Acknowledgments, Events (Access Granted, Access Denied, System/Alarm, Emergency/Duress, Area Anti-Passback), and Events Video Location **Record Types** are governed by the same **Records Older Than and Archive To** settings.

Some Events have associated video recordings, which are tracked in the Events Video Location table in the database. Video recordings, accumulated on video recorders, are periodically and/or continuously stored to some media by Video Archive Server. This activity is also tracked in the Events Video Location table. If Events are Archived/Purged, all not-stored (unarchived) video

recordings associated with these Events will no longer be noticed by the Video Archive Servers. They will therefore never be archived and will eventually take up all the storage space on the Video Recorders, causing them to stop recording.

In order to prevent this situation, the system verifies information about video recordings associated with Events being Archived/Purged. If any not archived video recordings are found, the user is prompted with two choices:

- Allow the system to request that the Video Archive Server archive all video recordings in question that match **Records Older Than** criteria and then continue with Archive/Purge.
- Cancel the Archive/Purge and change **Records Older Than** field for **Events and Alarm Acknowledgments** to a larger number (older video recordings are more likely to be archived).

Example:

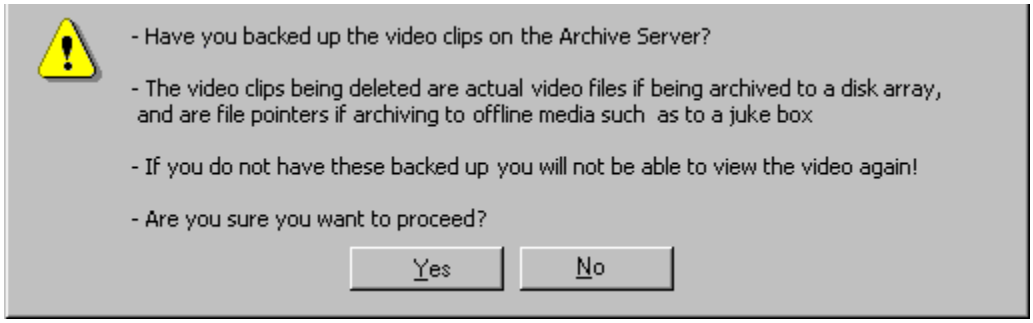
Notes: When Continuous Video records are archived or purged, their associated video recordings are deleted from online archived video storage. The records will be completely lost if you did not back up to offline storage before you began the archive or purge process. During the archive/purge process, the system will display a warning message. For example, the following warning message is displayed during a purge:

When Continuous Video records are archived or purged, their associated video recordings are DELETED from ONLINE archived video storage. They are COMPLETELY LOST if not already backed up to OFFLINE storage BEFORE the archive/purge process starts. System Administration posts warnings about this during the archive/purge process. For example, see the following warning that is displayed during a purge:

- When Events Video Location records are purged, their associated video recordings are deleted from online archived video storage. The records will be completely lost if you did not back up to offline storage before you began the archive/purge process.

  When Events Video Location records are archived, the system automatically forces the Video Archive Server to immediately archive any associated and not-yet-archived video recordings to online archived video storage.

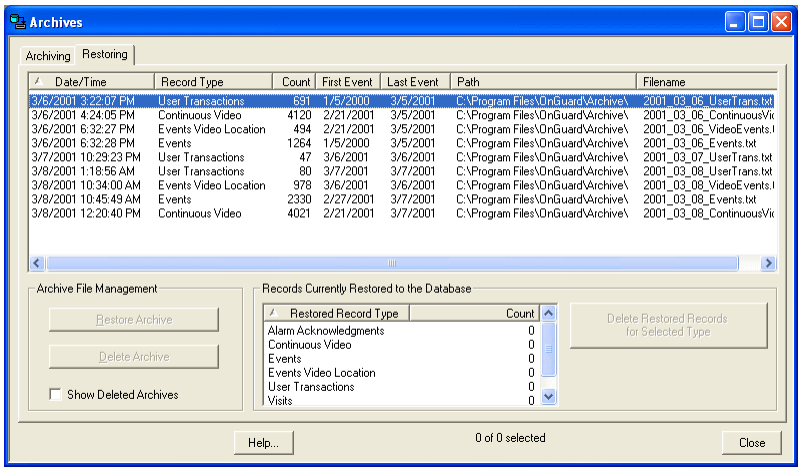
- Online archived video storage locations are specified on the Archive Server form of the Digital Video folder.
- Archive locations on DELL PowerVaults are considered to be ONLINE archived video storage. Customers can prevent the loss of video recordings stored in these locations by backing them up, either manually or automatically, via third-party backup software. The file folders specified for these archive locations need to be backed up ENTIRELY (i.e. the folders and all files and all sub-folders contained within them).
- During an archive/purge involving Events Video Location and/or Continuous Video records, the system will warn users with the following message before it deletes any associated video recordings from online archived video storage:



Restoring Form

This form is used to:

- View a list of all archive files that have been created.
- Restore records from an archive file to the database.
- Delete an archive file from the system.
- Delete restored records.



Listing window

Lists all archive files that have been created. Each (row) entry contains the following information

Date/Time - the date and time the file was created. EXAMPLE 1/8/00 1:23:54 PM

Record Type - the category of event, as listed on the Archiving form. For example: User Transactions

Count - the total number of events included in the file

First Event - the date of the oldest event included in the file. EXAMPLE 12/10/99

Last Event - the date of the most recent event included in the file. EXAMPLE 12/29/99

Path - the drive and directory in which the file resides. Specifically, it is the PurgeLog subdirectory of your application installation path.

Filename - the name of the text file that includes the archived events. The filename is derived from the date and the event type, and has the file extension “txt”.
EXAMPLE 2000_01_08_Visits.txt.

Files include:

- [date]AlarmAcks.txt - alarm acknowledgments
- [date]ContinuousVideo.txt - continuous video
- [date]Events.txt - user Transactions
- [date]EventsVideo.txt - user Transactions
- [date]UserTrans.txt - user Transactions
- [date]Visits.txt - user Transactions

Files created on previous OnGuard versions also include:

- [date]Area.txt - area anti-passback events
- [date]Denied.txt - access denied events
- [date]Duress.txt - emergency and duress events
- [date]Granted.txt - access granted events
- [date]System.txt - system and alarm events

Workstation - the name of the workstation from which the archive process was run

User - the user who created the file (archived the data)

Notes - if you delete an archive file, you are prompted to type any pertinent comments. Whatever you type is displayed here.

Archive File Management

Includes the [Restore Archive] and [Delete Archive] push buttons, and the **Show Deleted Archives** check box

Restore Archive

This button does not affect the actual archive (.txt) file stored in an archive directory. Instead, it copies the transactions from the selected archive file to a temporary/working table in the database. This table is not the same table as the one in which “live” (non-archived) transactions are stored. This is done so that restored records do not clutter the tables for current records. It allows you to quickly clear (remove the records from) a restored table without having to perform another archive/purge operation.

You can restore multiple archive files to the same working table. The **restored counts** value will be updated accordingly. If you try to restore an archive that cannot be located, you are prompted to browse for the file. You can navigate to a different drive/directory to find the file, but the filename itself must match the name stored in the database.

The browse feature is useful if you have moved files, or have backed them up and restored them to a different location. If you’ve deleted the archive file, you need to have made an accessible backup copy of the file in order to be able to restore its records.

Delete Archive

Deletes the selected archive file from the system. Its records are then permanently lost. For this reason it is advisable to back up an archive file before you delete it.

Show Deleted Archives

Even after an archive file has been deleted, you can display its listing window entry for historical reference. This applies to any archive file, no matter how long ago it was deleted. Remember, though, that the records contained in a deleted archive file are not retrievable (unless you've backed them up somewhere).

If this check box is selected, the listing window will include entries for deleted archive files. Entries for deleted files have the words "Delete Notes:" in the Notes column. If this check box is not selected, only archive files that have not been deleted will be listed.

Records Currently Restored to the Database

Includes the [Delete Restored Records] push button and the **restored counts** window.

Count

Indicates the number of records that have been restored to the database using the [Restore Archive] push button. This is the cumulative number of records currently stored in the temporary/working directories.

The window includes counters for Alarm Acknowledgments, Events (which includes access granted, access denied, system/alarm, emergency/duress, and area anti-passback events), Events Video Location, User Transactions, and Visit Records. A selected counter is reset to zero (0) when you click [Delete Restored Records].

Delete Restored Records for Selected Type

Clears the temporary/working table for the record type selected in the **restored counts** window (alarm acknowledgments, hardware events, or user transactions). The corresponding counter is reset to zero (0). This allows you to clear the restored records from a temporary database table so that you can "cleanly" restore another archive file.

Help

Displays pertinent help information on screen.

Mode

(view mode only) Indicates the record/selection count (such as "1 of 42 selected").

Close

Closes the Archives folder.

Restoring Form Procedures

The following procedures can be performed on this form.

Delete an Archive File From the System

Note: This procedure permanently removes an archive file from the system. If you haven't first backed up the file, you will be unable to restore it later, and the records will be lost. You cannot perform this procedure unless the **Delete Archive** check box is selected for

your user account on the Software Options sub-tab of the System Levels form in the Users folder.

1. In the listing window, highlight the archive file you wish to delete.
2. Click [Delete Archive].
3. The following message will be displayed: “If you have not backed up this file to another location, the information in this file will be lost. Are you sure you want to permanently delete the selected archive file?”

   Click [Yes] to proceed with deletion.

   Click [No] to cancel the request and to NOT delete the file.
4. If you selected [Yes] to proceed with deletion, the software then displays a Notes window in which you can type any relevant information that you want retained with the deletion record.

   In the Notes window, do one of the following:

   If you don’t want to delete the file, click [Cancel]. This is your last chance to back out of the process!

   If you do want to delete the file, enter any notes you wish to include, then click [OK].

   The archive file will be removed from the system. If you select the **Show Deleted Archives** check box, the entry for the archive file will be included in the listing window, and your delete notes will be displayed in the Notes column for that entry.

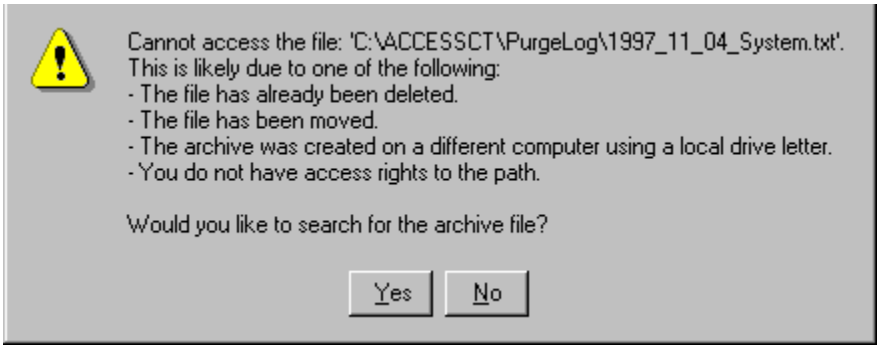
Restore Records to the Database

This procedure copies the records from the selected archive file to a temporary/working table in the database. You can do this only if the file still exists (i.e., if you have deleted the file and don’t have a backup, you’re out of luck). Note that you can perform this procedure only if the **Restore Transactions** check box is selected for your user account on the Software Options sub-tab of the System Levels form in the Users folder. Although this feature can be used to restore Continuous Video and Events Video Location records to the database, it does not restore any of their associated video recordings to online archived video storage. The system will attempt to restore an associated video recording to online archived video storage when a user attempts to play it via a Digital Video Player window in Alarm Monitoring.

1. In the listing window, highlight the archive file that contains the records you wish to restore.
2. Click [Restore Archive].
3. A message will be displayed indicating the number and type of record that will be restored to the database, and asking whether you wish to continue.
4. Click [Yes].
5. The application looks for the filename in the directory to which the file was archived. One of two things will happen:

   If the archive file is where it’s expected to be, a status indicator is displayed that tracks the progress of the restoration. A message is then displayed indicating how many events/records were restored successfully. The appropriate **record count** will be updated to include the newly restored events/records.

   If the archive file cannot be found, a message similar to the following will be displayed:



Click [Yes] to display an Open window, from which you can browse for the file. If you locate the file, click [Open] to initiate the restore.

Delete Restored Records From the Database

This procedure removes restored records from their temporary tables in the database. As long as the required archive files still exist, you can always restore the records again if you need to.

1. In the **restored counts** window, click on the counter you wish to clear—Alarm Acknowledgments, Events (which includes access granted, access denied, system/alarm, emergency/duress, and area anti-passback events), Events Video Location, User Transactions, and Visits.
2. Click [Delete Restored Records].
3. A message will be displayed asking whether you wish to delete all currently restored records of the selected type. Click [Yes]. The temporary table will be emptied and the selected counter will be reset to zero (0).

CHAPTER 24

Scheduler Folder

The Scheduler folder contains the Scheduler form with which you can schedule actions.

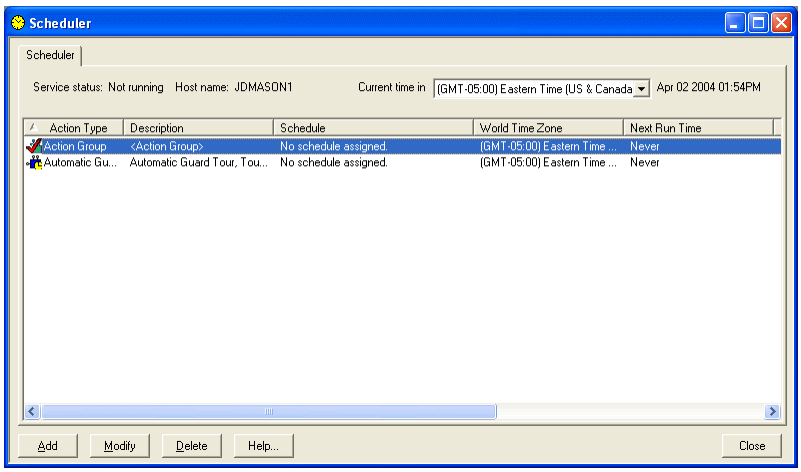
Additional documentation on actions is available in the Actions appendix. For more information please refer to Appendix A: Actions on page 1193.

This folder is displayed by selecting ***Scheduler*** from the ***Administration*** menu, or by selecting the Scheduler toolbar button.

Toolbar Shortcut

IMPORTANT: For the Scheduler to run and execute action the Linkage Server needs to be configured and running. You can configure the Linkage Server host on the General System Options Form on page 392.

Scheduler Form



Note: This form also displays in the Guard Tours Folder for your convenience.

Service status
Lists the status of the LS Linkage Server host and whether it's running or not. This is displayed only when the LS Linkage Server host is configured.

Host name
Lists the name of the host computer. This is displayed only when the Linkage Server host is configured.

Current time in
When scheduling an action, select which time zone you want the action to be scheduled in. The selections in the drop-down list are listed sequentially and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Listing window
Displays a list of all scheduled actions.

Add
Click this button to open the Add Action Wizard.

Modify
Click this button to modify the selected scheduled action.

Delete
Click this button to delete the selected scheduled action.

Help
Click this button to display online assistance for this form.

Close
Click this button to close the Scheduler folder.

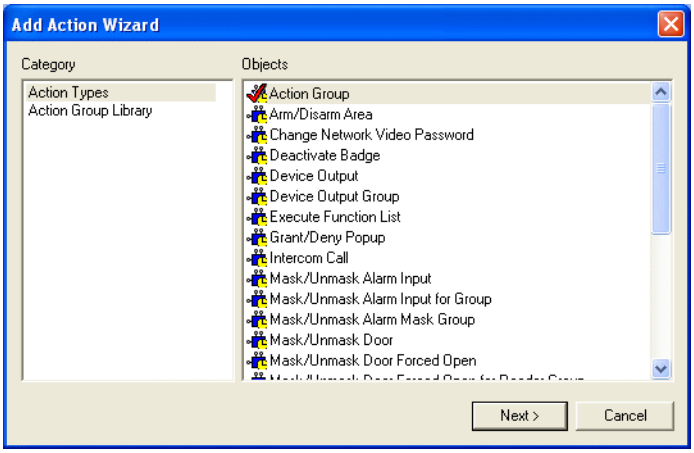
Scheduler Form Procedures

Use the following procedures on this form.

Add and Schedule an Action

1. Select ***Scheduler*** from the ***Administration*** menu. The Scheduler folder opens.
2. Click [Add]. The Add Action Wizard opens.

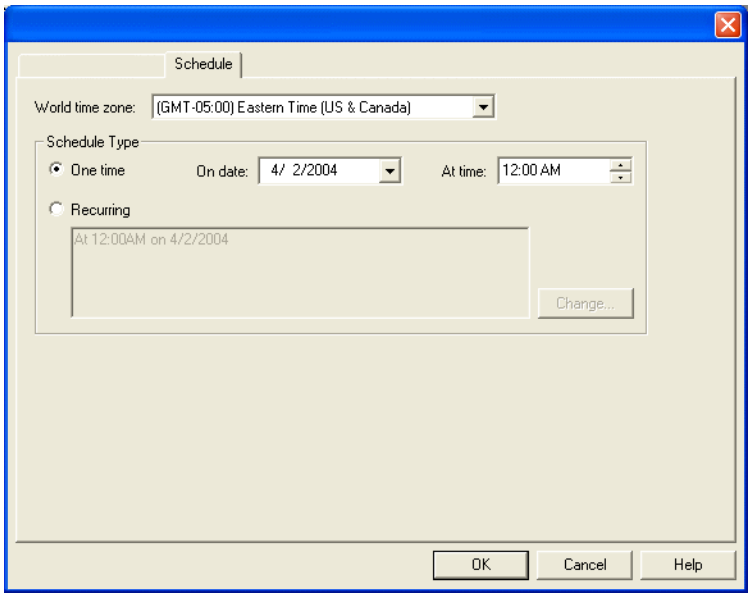
Note: You can also display the Add Action Wizard by right-clicking anywhere on the Scheduler form and selecting the ***Add Action*** menu option.



3. Select either “Action Types” or “Action Group Library” from the Category listing window.
   - When “Action Types” is selected, the Objects listing window lists all available action types.
   - When “Action Group Library” is selected, the Objects listing window lists all action groups which have been either created in or saved to the action group library. For more information, refer to Chapter 25: Action Group Library Folder on page 525.
4. Click on an entry in the Objects listing window to select it.
5. Click [Next]. Depending on which Category/Object combination you chose in steps 3 and 4, a corresponding action properties window will open.

   For example, if you selected “Action Types” in the Category listing window and “Archive/Purge Database” in the Objects listing window, then the Archive/Purge Database Properties window would open.
6. Click the Schedule tab. The Schedule form is displayed.

   The Schedule form is the same in every action properties window that is accessed via the Scheduler folder.



7. From the **World time zone** drop-down list, select which time zone you want the action to be scheduled in. The selections in the drop-down list are listed sequentially and each includes:

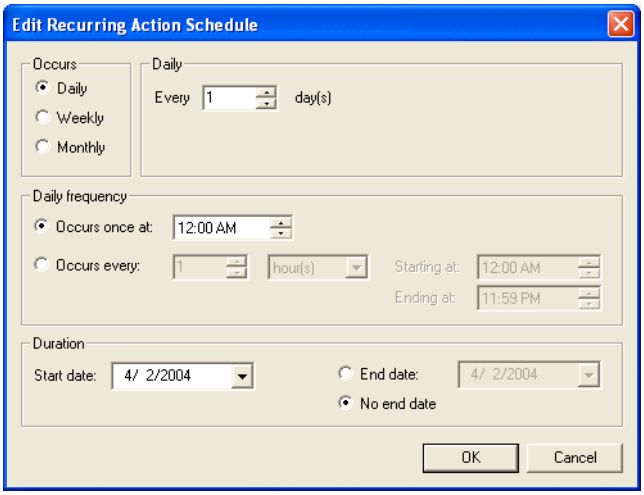
- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

8. If you want to schedule the action to occur more than once, skip this step and proceed to step 9. If you want to schedule the action to occur once:
   a. Select the **One time** radio button.
   b. In the **On date** field, the current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.

   - To select a month, click on the and navigation buttons.
   - You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
   - Navigate to a year by clicking on the displayed year to access the year spin buttons .
   - Once you have selected a month and a year, click on the day that you want the action to occur.

   c. In the **At time** field, select the time when you want this action to occur. Proceed to step 10.

9. If you want to schedule the action to occur more than once:
   a. Select the **Recurring** radio button.
   b. Click [Change]. The Edit Recurring Action Schedule window opens.



   c. Do one of the following:

- Select the **Daily** radio button in the Occurs section if you want the action to occur on a daily basis.

  If you want the action to occur every day, in the Daily section, type the number 1 in the **Every___day(s)** field. If you want the action to occur every other day, type the number 2 and so on.

- Select the **Weekly** radio button in the Occurs section if you want the action to occur on a weekly basis.

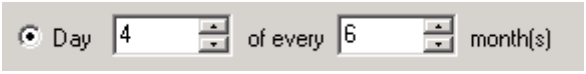
  If you want the action to occur every week, in the Weekly section, type the number 1 in the **Every___week(s) on** field. If you want the action to occur every other week, type the number 2 and so on. You must also select the check box that corresponds with the day of the week that you want the action to occur.

  For example, if you want the action to occur every other Monday, type the number 2 in the **Every___week(s) on** field and select the **Mon** check box.

- Select the **Monthly** radio button in the Occurs section if you want the action to occur on a monthly basis. Then, do one of the following:

  Select the **Day___of every___month(s)** radio button and type in which day of how many months you want the action to occur.

  The following example shows an action being scheduled to occur on the 4th day of every 6th month.

  Select the **The___of every___month(s)** radio button and enter which day of how many months you want the action to occur.

  The following example shows an action being scheduled to occur of the 2nd Tuesday of every 3rd month.

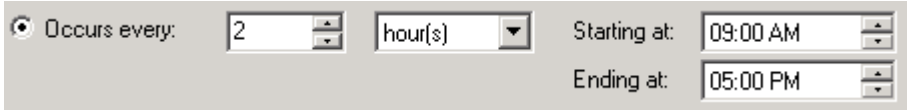
d. In the Daily frequency section, do one of the following:

- If you want the action to occur only once on its scheduled day(s), select the **Occurs once at___** radio button and enter a time.

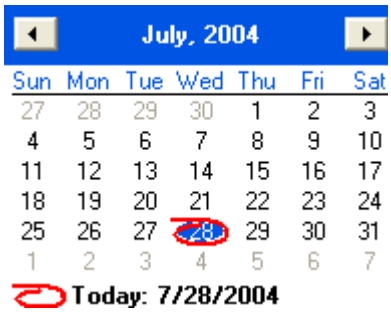
  The following example shows an action being scheduled to occur at 12:00 PM.

- If you want the action to occur more than once on its scheduled day(s), select the **Occurs every___Starting at___Ending at___** radio button and enter the hours that you want the action to occur.

  The following example shows an action being scheduled to occur every 2 hours, starting at 9:00 AM and ending at 5:00 PM.

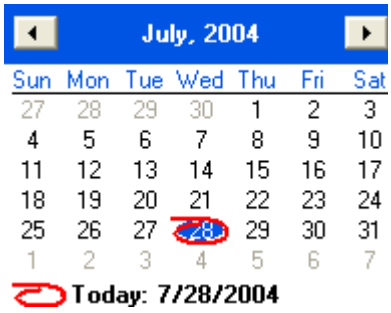
  

e. Enter the action's **Start date**. The current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.



- To select a month, click on the and navigation buttons.
- You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
- Navigate to a year by clicking on the displayed year to access the year spin buttons .
- Once you have selected a month and a year, click on the day that you want the action to begin occurring.

f. Enter the action's **End date**. The current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.



- To select a month, click on the and navigation buttons.
- You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
- Navigate to a year by clicking on the displayed year to access the year spin buttons .
- Once you have selected a month and a year, click on the day that you want the action to stop occurring.

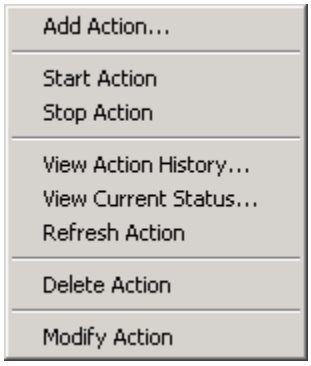
Note: You do not have to select an end date. If you do not want to set an end date, select the **No end date** radio button.

g. Click [OK].

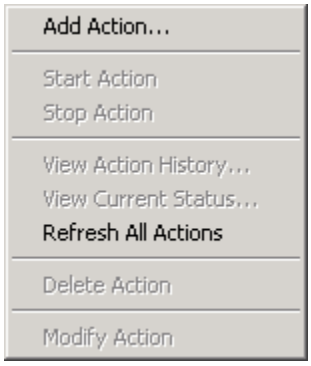
10. Now you must configure the action that you have just scheduled. Select the tab to the left of the Schedule tab (this tab will correspond to the specific action properties window which you are viewing). For more information please refer to Appendix A: Actions on page 1193.

Display the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.



Note: If you right-click anywhere on the Scheduler form when a scheduled action is not selected in the listing window, the scheduler right-click menu will look like this:



Add and Schedule an Action Using the Scheduler Right-Click Menu

1. Right-click anywhere on the Scheduler form. The scheduler right-click menu is displayed.
2. Select the ***Add Action*** menu option. The Add Action Wizard opens.
3. Proceed to step 3 of the "Add and Schedule an Action" procedure in this chapter.

Start an Action

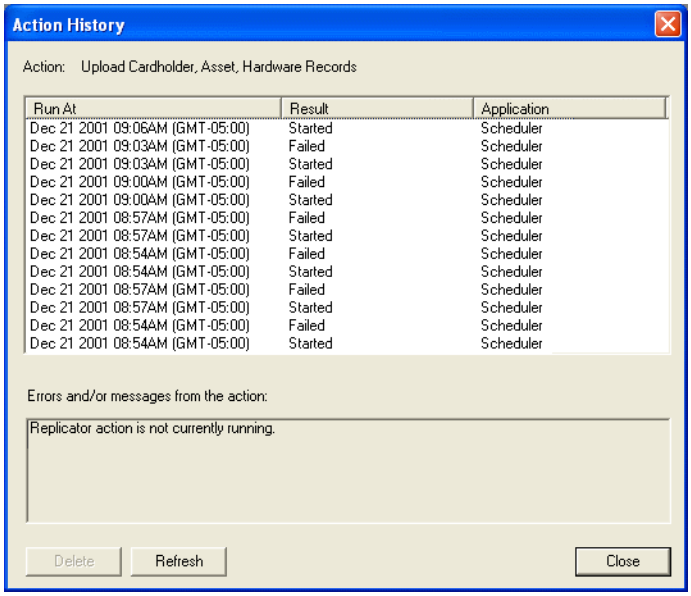
1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the ***Start Action*** menu option to start the selected action immediately.

Stop an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the ***Stop Action*** menu option to stop the selected action immediately.

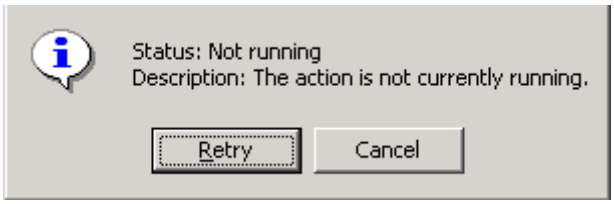
View Action History

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the ***View Action History*** menu option. The Action History window opens and the name of the action, when the action was run, the result, the application and any errors or messages that resulted from the action are all displayed.



View the Current Status of an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the ***View Current Status*** menu option. A message similar to the following will be displayed:



Refresh an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the ***Refresh Action*** menu option. The listing window will be updated to display the most current information for the selected action.

Refresh all Actions

1. Right-click anywhere on the Scheduler form except on a scheduled action in the listing window. The scheduler right-click menu is displayed.

2. Select the ***Refresh All Actions*** menu option. The listing window will be updated to display the most current information for all of the scheduled actions.

Delete a Scheduled Action using the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the ***Delete Action*** menu option. A confirmation message is displayed.
3. Click [Yes].

Note: Selecting the ***Delete Action*** right-click menu option does the same thing as selecting an action in the listing window, and then clicking [Delete] on the Scheduler form.

Modify a Scheduled Action using the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the ***Modify Action*** menu option. Depending on which action you selected in the listing window, a corresponding action properties window will open.
3. Make the changes you want to the fields. For more information please refer to Appendix A: Actions on page 1193.
4. Click [OK].

Note: Selecting the ***Modify Action*** right-click menu option does the same thing as selecting an action in the listing window, then clicking the [Modify] button on the Scheduler form.

CHAPTER 25

Action Group Library Folder

The Action Group Library folder contains the Action Group Library form with which you can create, modify, and delete action groups.

This folder is displayed by selecting ***Action Group Library*** from the ***Administration*** menu, or by selecting the Action Group Library toolbar button.

Toolbar Shortcut

Action Groups Overview

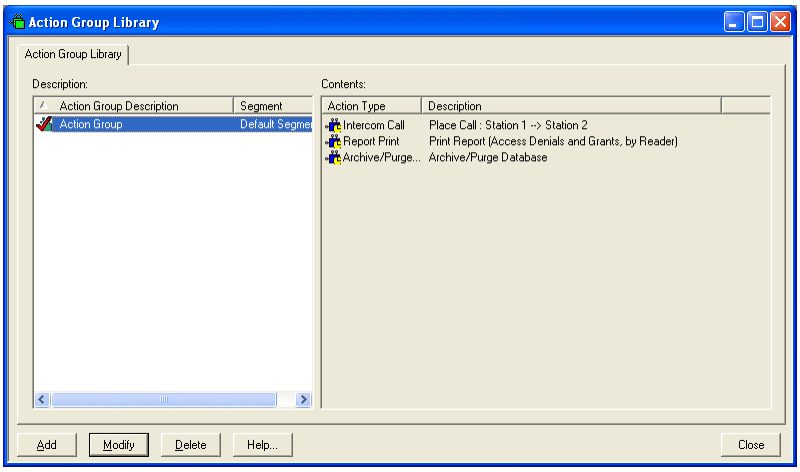
Note: You must refer to the Actions appendix for detailed information on actions. For more information please refer to Appendix A: Actions on page 1193.

The purpose of the Action Group Library folder is to create action groups.

An *Action Type* is any task that can be performed by the system as a result of an event or a schedule. All actions are organized by action types. **Action Group** is one action type.

An *Action Group* is a group of actions that will be executed simultaneously. Once an action group is created, it can be used by other System Administration features. For example: when assigning actions in the Guard Tour folder, you can assign an action group that was created in the Action Group Library folder.

Action Group Library Form



Description listing window

Lists all action groups that have been created. A icon precedes each action group entry.

Contents listing window

Lists all actions that belong to the selected action group. A icon precedes each entry.

Add

When selected, displays the Action Group Properties window from where you can add an action group.

Modify

When selected, displays the Action Group Properties window from where you can modify an existing action group.

Delete

When selected, removes the selected action group from the system.

Help

When selected, displays online help information for this form.

Close

Closes the Action Group Library folder.

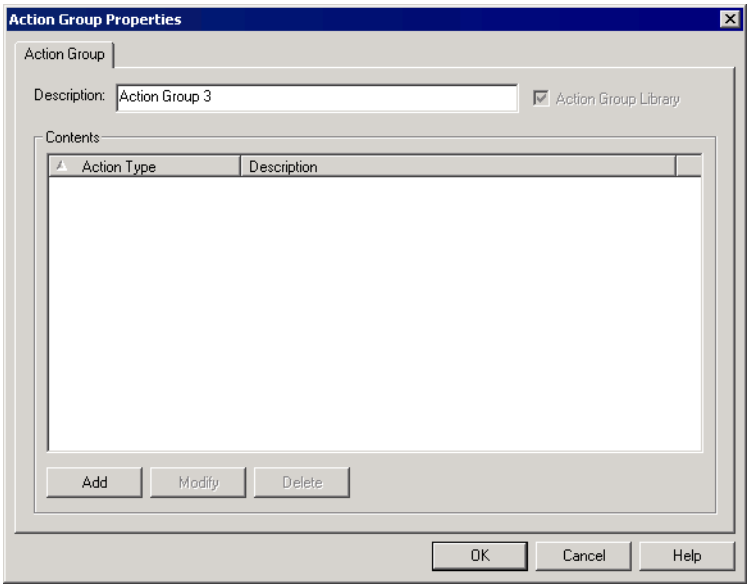
Action Group Library Form Procedures

The following procedures can be performed on this form.

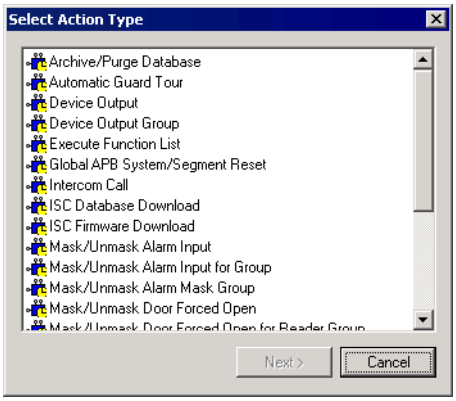
Add an Action Group

1. Select ***Action Group Library*** from the ***Administration*** menu. The Action Group Library folder opens.
2. Click [Add]. If segmentation is not enabled on your system, proceed to step 4.

3. If segmentation is enabled on your system, the Segment Membership window opens. Select a segment and click [OK].
4. The Action Group Properties window opens. In the **Description** field, type a name for the action group.



5. Click [Add]. The Select Action Type window opens.



6. From the listing window, click on an action type to select it.
7. Click [Next]. Depending on which action type you chose in step 6, a corresponding action type properties window will open.

   You must refer to the Actions appendix in this user guide for detailed information on how to use the action type properties windows to assign an action. For more information please refer to Appendix A: Actions on page 1193.
8. Repeat steps 5-7 for each action you want to assign to this action group.
9. Click [OK].

Modify an Action Group

1. In the Description listing window, click on the name of the action group that you want to modify.
2. Click [Modify]. The Action Group Properties window opens.

3. If you want to modify an action type that has already been assigned to the selected action group, in the Contents listing window, click on an assigned action type to select it.
4. Click [Modify]. Depending on which action type you chose in step 3, a corresponding action type properties window will open.

   You must refer to the Actions appendix in this user guide for detailed information on how to use the action type properties windows to modify an assigned action. For more information please refer to Appendix A: Actions on page 1193.
5. Repeat steps 3 and 4 to for each assigned action type that you want to modify.
6. To assign an action type to this action group, click [Add]. The Select Action Type window opens.
7. From the listing window, click on an action type to select it.
8. Click [Next]. Depending on which action type you chose in step 7, a corresponding action type properties window will open.

   You must refer to the Actions appendix in this user guide for detailed information on how to use the action type properties windows to assign an action. For more information please refer to Appendix A: Actions on page 1193.
9. Repeat steps 6-8 for each action you want to assign to this action group.
10. Click [OK].

Delete an Action Group

1. In the Description listing window, click on the name of the action group that you want to delete.
2. Click [Delete]. An Action Group Library Configuration deletion confirmation message is displayed.
3. Click [Yes].

CHAPTER 26

Global Output Devices Folder

The Global Output Devices folder contains forms with which you can:

- Define SMTP server settings to be used when sending electronic mail messages via the global output server.
- Define a GOS paging device to be used when sending pager messages via the global output server.
- Define all prospective recipients of e-mail and pager messages.

The folder contains three forms: the SMTP Server Settings form, the Paging Devices form, and the Recipients form.

The Global Output Devices folder is displayed by selecting ***Global Output Devices*** from the ***Administration*** menu, or by selecting the GOS Devices toolbar button.

Toolbar Shortcut

Global Output Server Overview

The Global Output Server (GOS) feature supports on-demand messaging from Alarm Monitoring. Functionally, an Alarm Monitoring user (such as a security guard) can send an electronic mail or pager message pertaining to a specific alarm displayed on his/her workstation.

Behind the scenes, the GOS client (i.e., Alarm Monitoring) sends the message to GOSServer (which runs as a Windows operating system service). GOSServer then directs the message to the appropriate Global Output Device.

- If the message is a page, the paging software then sends it to the recipient via the paging service or in-house paging terminal.
- If the message is electronic mail, the electronic mail server then sends it to the recipient via the electronic mail service.

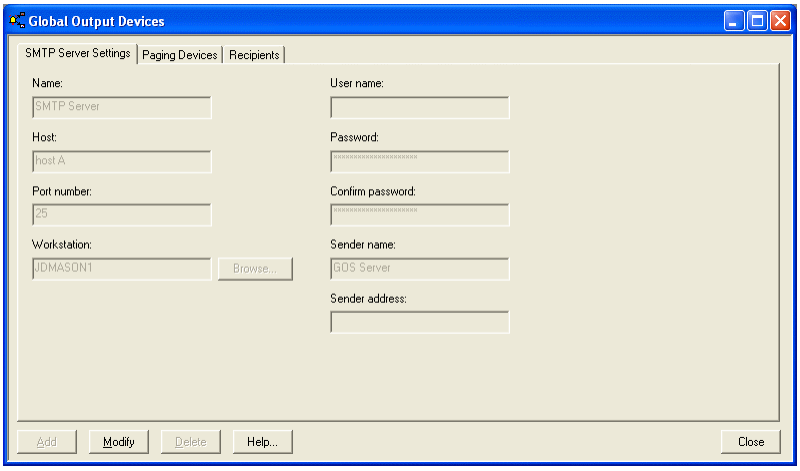
To use this feature you must first:

- Purchase, install, and configure the electronic mail and/or paging software.
- Use this folder to configure the SMTP server settings or paging devices and the message recipients. You define such a device to be on the workstation where the associated application (for example, the e-mail or paging software) resides. If you have both a paging application and an electronic mail application, they may have been installed on two different computers.
- Launch the Global Output Server application, which is located in the OnGuard program group. Like the Communication Server, Global Output Server runs in the background, but it must be active in order to send messages from Alarm Monitoring. For more information, refer to the Alarm Monitoring User Guide.

Specifications

	E-Mail	Paging
Output Devices:	SMTP server	Wireless paging software
Message Types:	ASCII (plain) text only	Alphanumeric
Recipient Addresses:	Any address that can be correctly resolved and handled by your electronic mail server	Any alphanumeric pager that can be accessed through a paging terminal with your wireless paging software can communicate using the TAP (Telocator Alphanumeric Protocol).

SMTP Server Settings Form



Name

Enter a descriptive name for the SMTP server.

Host

Specify the host computer for the SMTP server.

Port number
Specify the port that is on the serial expansion unit or the back of the host server.

Workstation
Identifies the workstation on which the global output server applications is running on. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse
Displays a Browse for Computer window from which you can click on the name of a workstation to highlight the entry. Click [OK] to then enter the workstation name in the **Workstation** field.

User name
In modify mode, enter a user name if the SMTP server's authentication level requires it.

Password
If a user name was entered in the **User name** field, type in a password. Your password is not displayed as you type.

Confirm password
Enter here exactly the same information that you entered in the **Password** field.

Sender name
Enter the sender's name. The default is "GOS Server."

Sender address
Enter the sender's address. The address must be in SMTP format. For example, "administration@company.com." Although it is not required, it is highly recommended that you enter a sender address. Some systems may require a valid e-mail address or for security reasons, may require that the address belong to a certain domain name.

Modify
Click on this button to configure SMTP server settings.

Help
Click this button to display online help for this form.

Close
Click this button to close the Global Output Devices folder.

SMTP Server Settings Form Procedures

Use the following procedures on this form.

Configure SMTP Server Settings

1. Select ***Global Output Devices*** from the ***Administration*** menu.
2. Click [Modify].
3. Enter a descriptive **Name** for the SMTP server.

4. Specify the **Host** computer and the **Port** that is on the serial expansion unit or the back of the host server.
5. Enter the **Workstation** on which the global output server applications have been installed. You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Note: You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

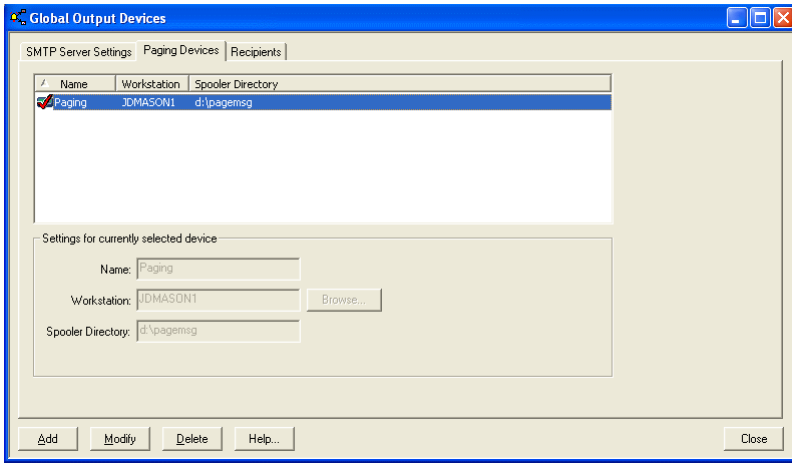
6. If the SMTP server's authentication level requires it:
   a. Enter a **User Name** and **Password**.
   b. In the **Confirm Password** field, enter here exactly the same information that you entered in the **Password** field.
7. Enter the **Sender Name**. The default is "GOS Server."
8. Enter the **Sender Address**. The address must be in SMTP format. For example, "administration@company.com."

Note: Although it is not required, it is highly recommended that you enter a sender address. Some systems may require a valid e-mail address or for security reasons, may require that the address belong to a certain domain name.

9. Click [OK].

Paging Devices Form

This form is used to define a GOS paging device to be used when sending pager messages via the Global Output Server.



Listing window

Lists all Paging devices currently defined in the application. Each entry is preceded by a icon, and includes the device's **Name**, **Workstation**, and **Spooler Directory**.

Settings for Currently Selected Device

Includes the **Name**, **Workstation**, and **Spooler Directory** fields.

Name
Enter a unique, descriptive name for the Paging device.

Workstation
Identifies the workstation on which the Paging and Global Output Server applications have been installed. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse
Displays a Browse for Computer window from which you can click on the name of a workstation to highlight the entry. Click [OK], and then enter the workstation name in the **Workstation** field on the Paging form.

Spooler Directory
Specify the location of the wireless paging software's spooler directory on the **Workstation**. Functionally, a Paging message sent from the Global Output Server is temporarily stored in the spooler directory. The wireless paging software then retrieves the message from the spooler directory and forwards it to the designated recipient.

Add
Click on this button to add a Paging device.

Modify
Click on this button to change the selected Paging device.

Delete
Click on this button to delete the selected Paging device.

Help
Displays online help for this form.

Mode
In modify mode, indicates the current operation, such as "Modify Mode".

Close
Closes the Global Output Devices folder.

Paging Devices Form Procedures

Use the following procedures on this form.

Add A Paging Device

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for the paging device.
3. In the **Workstation** field, enter the name of the computer on which the wireless paging software and the Global Output Server software have been installed.

Notes: This **Workstation** must be the same computer that was specified in the wireless paging software.

You are required to enter the workstation's NetBIOS name. The NetBIOS name is specified when Windows networking is installed/configured.

4. In the **Spooler Directory** field, type the directory on the **Workstation** in which temporary page messages will be stored.

Note: This must be the same directory that is specified in the wireless paging software.

5. Click [OK]. In the listing window, an entry will be added for the Paging device.

Modify a Paging Device

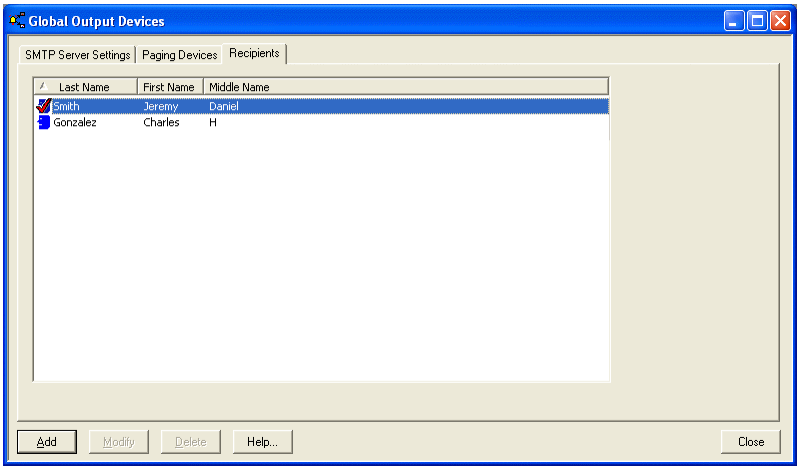
1. In the listing window, select the name of the Paging device you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Paging Device

1. In the listing window, select the name of the Paging device you wish to delete.
2. Click [Delete].
3. Click [OK].

Recipients Form

This form is used to define all potential recipients of e-mail and paging messages.



Listing window

Lists all currently defined Global Output Server recipients. Each entry is preceded by a icon, and includes the person's **Last Name**, **First Name**, and **Middle Name**.

Add
Click on this button to add a recipient.

Modify
Click on this button to change information for the selected recipient.

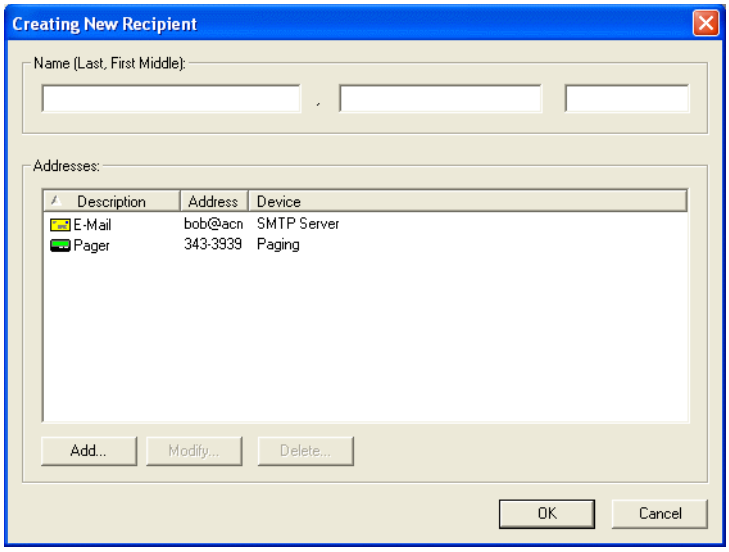
Delete
Click on this button to delete the selected recipient record.

Help
Displays online help for this form.

Close
Closes the Global Output Devices folder.

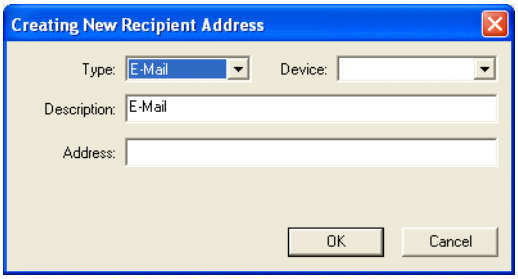
Creating New [Modifying] Recipient Window

This window is displayed by clicking the [Add] or [Modify] button on the Recipients form.



Creating New [Modifying] Recipient Address Window

This window is displayed by clicking the [Add] or [Modify] button on the Adding [Modifying] Recipient window.



Name
Includes the **Last Name**, **First Name**, and **Middle Name** fields.

last name
Enter the recipient's last name.

first name
Enter the recipient's first name.

middle name
Enter the recipient's middle initial or name.

Addresses
Lists all currently defined addresses for this recipient. Each entry is preceded by a or a icon and includes a description, the actual address, and whether it is an e-mail or pager address.

Add
Click on this button to add a recipient address.

Modify
Click on this button to change the selected address.

Delete
Click on this button to delete the selected address.

OK
Saves changes and returns you to the Recipients form.

Cancel
Cancels pending changes and returns you to the Recipients form.

Type
Indicate whether the address you're adding or modifying is to be used for electronic mail or paging. Choose either "E-Mail" or "Pager."

Device
Indicates the global output device to be used for messages to this recipient. Choices include all currently defined devices of the **Type** you selected. (The only device available for e-mail is "SMTP Server" and devices listed for the pager type are defined on the Paging Devices form.) If more than one device has been defined for the specified **Type**, you can select the one you want to use for this recipient.

Description
The application automatically enters either "E-Mail" or "Pager" here, based upon your **Type** field selection. You can, however, modify this default value. Type a description to distinguish this address from the recipient's other addresses (if any). For example, "Personal E-Mail" or "Technical Support Pager"

Address
Specify the actual e-mail or paging address.

For e-mail: type the address exactly as required to send messages to the recipient. For example, kdsmith@aol.com

For paging: the required syntax is: <recipient's pager PIN number>.<paging service name> For example, 20234.ZippyPage

A pager's PIN is assigned by the paging carrier company. Paging service names (carriers) are defined in the wireless paging software, and correspond to paging carrier companies or an in-house paging terminal. The combination of the PIN and paging service name uniquely identifies each pager.

OK

Saves changes and returns you to the Creating New [Modifying] Recipient window.

Cancel

Cancels pending changes and returns you to the Creating New [Modifying] Recipient window.

Recipients Form Procedures

Use the following procedures on this form.

Add a Recipient

1. Click [Add].
2. In the Creating New Recipient window, type the recipient's name directory-style. In other words, enter the last name first, followed by first name then middle name or initial. Press the <Tab> key to move between the fields.
3. To add e-mail and paging addresses for the recipient:
   a. Click [Add] in the Creating New Recipient window.
   b. In the Creating New Recipient Address window, choose the address **Type** ("E-Mail" or "Pager").
   c. The application then assigns default **Device** and **Description** values automatically. You may want to change these, especially if multiple devices are defined or if the recipient has multiple addresses. (The only device available for e-mail is "SMTP Server" and devices listed for the **Pager** type are defined on the Paging Devices form.)
   d. Type the actual e-mail or page **Address**. The address depends on the carrier settings in the Emergin Orchestrator program.
   e. Repeat steps a-d for each additional address to be defined for this recipient. The person might have an office pager plus office and home e-mail addresses, for example.
   f. Click [OK] to close the Creating New Recipient Address window.
4. Click [OK] to close the Creating New Recipient window. The recipient's name will be added to the listing window on the Recipients form.

Modify a Recipient

1. In the listing window, select the name of the recipient record you wish to change.
2. Click [Modify].
3. Make the changes you want. You can change the recipient's name, add other addresses, or change or remove a selected address.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Recipient

1. In the listing window, select the name of the recipient record you wish to delete.
2. Click [Delete].
3. Click [OK].

Access Control

CHAPTER 27

Access Panels Folder

The Access Panels folder contains forms with which you can:

- Name individual access panels in the software
- Specify access panel setup parameters, including information stored in the panel
- Specify communication panel setup parameters, including the workstation associated with the panel
- View the firmware, DIP switch settings and flash chip size of LNL-3300, 2220, 2210, 2000, 1000, or 500 panels
- Enable encryption on LNL-3300, 2220, 2210, 2000, 1000, or 500 panels, if the system/segment is configured for encryption and you have the proper user permission

The folder contains several forms, the LNL-3300 form, LNL-2220 form, LNL-2210 form, LNL-2000 form, the LNL-1000 form, the LNL-500 form, the HID form, and the Other form.

Toolbar Shortcut

The Access Panels folder is displayed by selecting ***Access Panels*** from the ***Access Control*** menu, or by selecting the Access Panels toolbar button.

NGP Form Overview

For more information please refer to Appendix L: NGP Access Panel Configuration on page 1527.

ILS Forms Overview

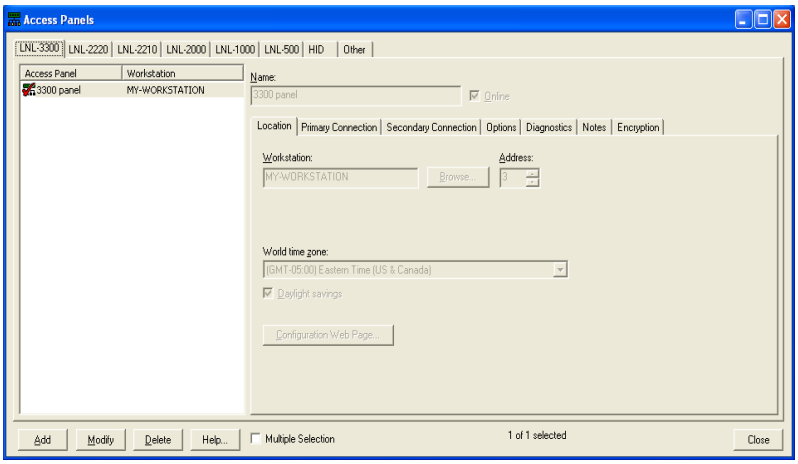
For more information on configuring the ILS Integra, ILS Offline, and ILS Wireless access panels, refer to Appendix K: Lenel ILS (Integrated Locking Solutions) on page 1473..

LNL-3300 Form Overview

This form is used to:

- Assign names to individual LNL-3300 type access panels in the software
- Specify access panel setup parameters, including information stored in the panel
- Specify communication panel setup parameters, including the workstation associated with the panel and the access method (direct serial connection, LAN, or dialup)
- View the firmware, DIP switch settings and flash chip size of the panel
- Enable encryption, if you have the proper user permission

LNL-3300 Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the access panel. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Selects the workstation or server to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

Address

Specifies the panel's address, which must match the DIP switch setting on the panel itself. Possible values are in the range of 0 through 7. The factory default DIP switch setting is 0. For any panel(s) that will be communicating with a workstation using a dialup connection, the panel(s) must be set to address 1 or the dial-back to host capability will fail.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Configuration Web Page

Opens the web page used to configure the access panel. Only available when in view mode and if the controller has an IP address or host name configured for the primary connection.

Add

Adds a panel entry.

Modify

Changes a panel entry.

Delete

Removes a panel entry.

Help

Displays online help for this topic.

Change Segment

Displays if segmentation is enabled and you are in modify mode. Click this button to move the access panel to a different segment.

Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected panels.

Mode

In view mode, indicates how many panels are currently selected, and the current total number of panels; for example, "2 of 5 selected".

In modify mode, indicates the current operation (Add Mode, Modify Mode, etc.).

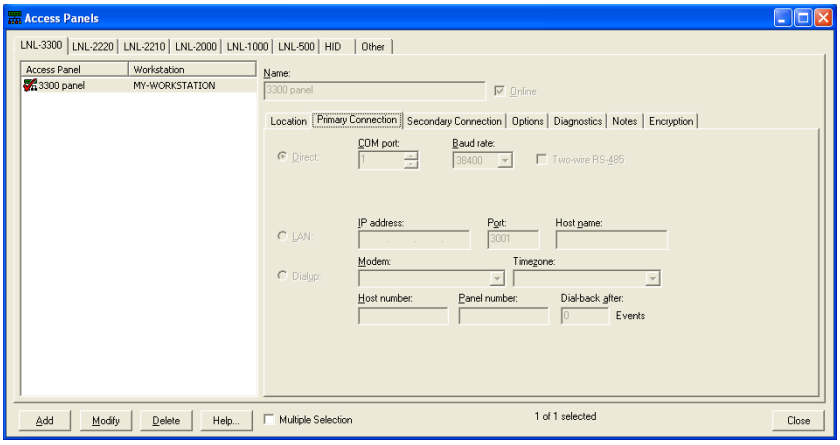
Close

Closes the Access Panels folder.

LNL-3300 Form (Primary Connection Sub-tab)

Certain options on the Primary Connection and Secondary Connection tabs function together to limit combinations of primary and secondary communications for dual path usage. Valid dual path selections include:

Primary Connection option selected	Secondary Connection options available for selection
Direct	None and LAN
LAN	None, Direct, LAN, Dialup
Dialup	Secondary connection not allowed.



Direct

Select this radio button if communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**, the **Baud rate**, and whether or not communication to the host will use a **Two-wire RS-485** connection.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 through 255.

Baud rate

If you selected the **Direct** radio button, this is the speed (in bits per second) at which information is transferred between the workstation and the access panel via the serial connection.

Note: Some third party devices do not allow the baud rate to be modified from the host application software. If such a device is in use, the baud rate setting in OnGuard has no bearing. Refer to the documentation for any third party devices being used.

Two-wire RS-485

Other panels can be configured to communicate with the host workstation using either a 4-wire or 2-wire RS-485 connection. Select this check box if 2-wire communication is to be used.

LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's IP address or Host name.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Port

The network port that the LAN connection will be established on. This needs to match what is specified in the LNL-3300 configuration web page. The default is 3001.

Host Name

The host name that the LNL-3300 will use with DHCP and will register with the DHCP server. Instead of referencing the panel by a static IP address you may be able to reference it by the host name depending on your network configuration.

Dialup

Select this radio button if the workstation will communicate with the access panel using a dialup connection. This option functions together with the LAN option on the Secondary Connection sub-tab to limit combinations of primary and secondary communications for dual path usage. You must also specify the workstation's modem, timezone, host number, panel number and dial-back after__events.

Modem

If you selected the **Dialup** radio button, select the modem on the workstation that will be used for dialup communication with the access panel. Choices include all TAPI (Telephone Application Programming Interface) devices that are currently configured on the specified Workstation.

Before a modem can be listed in this drop-down list, the modem must be properly configured for the selected workstation. This is done on the Modems form in the Dialup Configuration folder, which is reached by selecting ***Modems*** from the ***Access Control*** menu. For more information, refer to Connect a Modem to a Lenel Access Panel on page 704.

If any of the TAPI devices are used for other dial functions such as remote access, do not select them for panel dial usage.

For more information, refer to your Windows user guide.

Timezone

If you selected the **Dialup** radio button, indicate the timezone during which the access panel will initiate dialup communication with the workstation. You can select only one timezone for the particular workstation-modem-panel combination. Timezones are defined on the Timezones form of the Timezones folder.

Functionally, at the start of each interval that comprises the timezone, the panel will automatically dial the host number. If a connection cannot be established, it will redial until a connection can be made. Once connected, all transactions stored in the panel will be dumped to the Communication

Server (on the workstation) to be logged in the database. In addition, all commands that need to be sent to the panel will be sent from the host at that time.

After all information is transferred, the Communication Server will automatically terminate the dialup connection with the panel. The exception to this occurs if you select the “Always” timezone. In that situation, the workstation will attempt to always stay connected to the panel via dial-up. Functionally, this is similar to communicating with the workstation via a direct (serial) or LAN connection.

Multiple workstations can use the same TAPI modem, or one workstation might have access to multiple TAPI modems. However, only one connection to a particular modem can be established at a particular time. For example, a particular workstation might use a particular modem to dial one panel at 12:00, a second panel at 1:00, a third panel at 2:00, etc.

Host number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that’s connected to the workstation. This is the number that the access panel will use to dial into the panel to send events and other transactions to the workstation.

Type the exact dialing sequence here. Although you can use parentheses and dashes, they are ignored by TAPI devices. For example, 2489720 and (212) 546-1234. For more information, refer to your Windows user guide.

Panel number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that’s connected to the access panel. This is the number that the workstation would need to dial to communicate with the access panel.

Typically, all communication between the access panel and the workstation is initiated from the panel. However, the workstation can dial the panel from within the Alarm Monitoring system. This is done by right-clicking on the panel’s entry in the System Tree, then selecting the **Connect** command from the popup menu.

Any ASCII string can be typed here (for example, a comma typically triggers a pause in the dialing sequence).

Dial-back after__Events

This field is displayed only if you have selected the **Dialup** radio button.

LNL-3300 panels can be programmed to dial the workstation after a certain number of events have been stored in the panel but have not yet been reported to the host (because the panel has been offline).

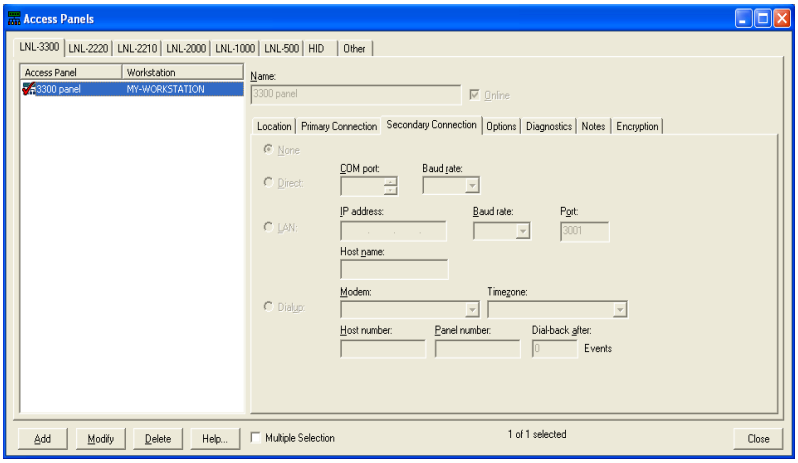
When the panel has accumulated the specified number of stored events, the panel will automatically dial the host number to dump its transactions and to receive any command programming. After the information has been exchanged, the workstation will terminate the connection.

The default value here is 255 events. The minimum value you can enter is zero (meaning that the panel will never dial the host). The maximum value is equal to one less than the maximum number of events that the panel can store.

LNL-3300 Form (Secondary Connection Sub-tab)

Certain options on the Secondary Connection and Primary Connection tabs function together to limit combinations of secondary and primary communications for dual path usage. Valid dual path selections include:

Secondary Connection option selected	Primary Connection options available for selection
Direct	None and LAN
LAN	None, Direct, LAN, Dialup
Dialup	Secondary connection not allowed.



None

Select if you want no secondary connection.

Direct

Select this radio button if for the secondary connection, communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 through 255.

LAN

Select this radio button if for the secondary connection the workstation will communicate with the access panel over a Local Area Network. This option functions together with the **Dialup** option on the Primary Connection sub-tab to limit combinations of primary and secondary communications for dual path usage. You must also specify the workstation's **IP address or Host name**.

IP address

If you selected the **LAN** radio button for secondary connection, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP

address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Baud rate

If you selected the **Direct** or **LAN** radio button, this field displays the speed (in bits per second) at which information is transferred between the workstation and the access panel via the serial connection. A baud rate of 38400 is automatically entered into this field when a **LAN** connection is selected. This value cannot be changed.

Note: Some third party devices do not allow the baud rate to be modified from the host application software. If such a device is in use, the baud rate setting in OnGuard has no bearing. Refer to the documentation for any third party devices being used.

Port

The network port that the LAN connection will be established on. This needs to match what is specified in the LNL-3300 configuration web page. The default is 3001

Host Name

The host name that the LNL-3300 will use with DHCP and will register with the DHCP server. Instead of referencing the panel by a static IP address you may be able to reference it by the host name depending on your network configuration.

Dialup

Select this radio button if for the secondary connection the workstation will communicate with the access panel using a dialup connection. You must also specify the workstation's **Modem**, **Timezone**, **Host number**, **Panel number** and **Dial-back after__Events**.

Modem

If you selected the **Dialup** radio button for secondary connection, select the modem on the workstation that will be used for dialup communication with the access panel. Choices include all TAPI (Telephone Application Programming Interface) devices that are currently configured on the specified **Workstation**.

Before a modem can be listed in this drop-down list, the modem must be properly configured for the selected **Workstation**. This is done on the Modems form in the Dialup Configuration folder, which is reached by selecting ***Modems*** from the ***Access Control*** menu. For more information, refer to Connect a Modem to a Lenel Access Panel on page 704.

If any of the TAPI devices are used for other dial functions such as remote access, do not select them for panel dial usage.

For more information, refer to your Windows user guide.

Timezone

If you selected the **Dialup** radio button for secondary connection, indicate the timezone during which the access panel will initiate dialup communication with the workstation.

You can select only one timezone for the particular workstation-modem-panel combination. Timezones are defined on the Timezones form of the Timezones folder.

Functionally, at the start of each interval that comprises the timezone, the LNL-3300 panel will automatically dial the **Host number**. If a connection cannot be established, it will redial until a connection can be made. Once connected, all transactions stored in the LNL-3300 will be dumped to the Communication Server (on the workstation) to be logged in the database. In addition, all commands that need to be sent to the LNL-3300 will be sent from the host at that time.

After all information is transferred, the Communication Server will automatically terminate the dialup connection with the LNL-3300 panel. The exception to this occurs if you select the "Always" timezone. In that situation, the workstation will attempt to always stay connected to the panel via dial-up. Functionally, this is similar to communicating with the workstation via a direct (serial) or LAN connection.

Multiple workstations can use the same TAPI modem, or one workstation might have access to multiple TAPI modems. However, only one connection to a particular modem can be established at a particular time. For example, a particular workstation might use a particular modem to dial one panel at 12:00, a second panel at 1:00, a third panel at 2:00, etc.

When the "Always" timezone is used as the dialup timezone for the secondary connection, the primary connection needs to be non-dialup (direct or LAN). When the primary connection is up, the secondary connection will be offline. If the primary connection goes down, a call will be placed to the panel on the secondary path after a certain period of time (default roughly 60 seconds). Once the secondary dialup connection has been established, the connection will remain until the primary connection has been re-established. After the primary connection is established, the secondary connection will remain connected for about one to two minutes (to make sure that the primary connection has connected and remained connected).

Host number

If you selected the **Dialup** radio button for secondary connection, enter the phone number used to reach the modem that's connected to the workstation. This is the number that the access panel will use to dial into the panel to send events and other transactions to the workstation.

Type the exact dialing sequence here. Although you can use parentheses and dashes, they are ignored by TAPI devices.

For example, 2489720 and (212) 546-1234. For more information, refer to your Windows user guide.

Panel number

If you selected the Dialup radio button for secondary connection, enter the phone number used to reach the modem that's connected to the access panel. This is the number that the workstation would need to dial to communicate with the access panel.

Typically, all communication between the access panel and the workstation is initiated from the panel.

However, the workstation can dial the panel from within the Alarm Monitoring system. This is done by right-clicking on the panel's entry in the System Tree, then selecting the Connect command from the popup menu.

Any ASCII string can be typed here (for example, a comma typically triggers a pause in the dialing sequence).

Dial-back after__Events

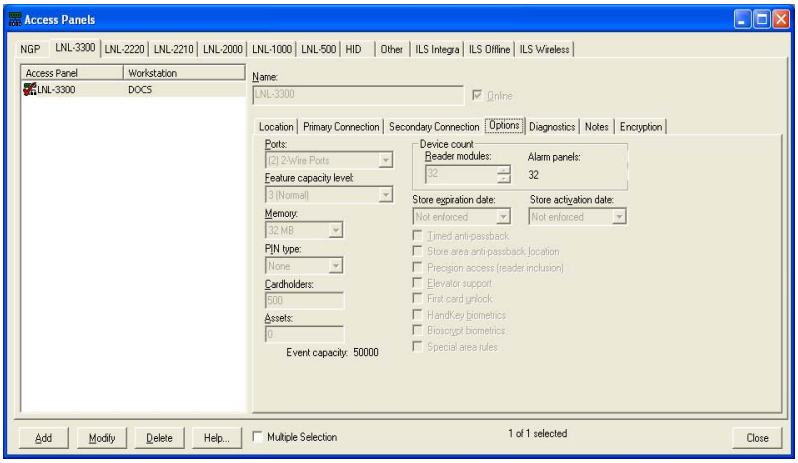
This field is displayed only if you have selected the Dialup radio button for secondary connection.

LNL-3300 panels can be programmed to dial the workstation after a certain number of events have been stored in the panel but have not yet been reported to the host (because the panel has been offline).

When the panel has accumulated the specified number of stored events, the panel will automatically dial the Host Number to dump its transactions and to receive any command programming. After the information has been exchanged, the workstation will terminate the connection.

The default value here is 255 events. The minimum value you can enter is zero (meaning that the panel will never dial the host). The maximum value is equal to one less than the maximum number of events that the panel can store.

LNL-3300 (Options Sub-tab)



Note: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

Ports

Access panels communicate with its *downstream devices* (reader interfaces, input control modules, and output control modules) using either 2- or 4-wire RS-485 communication, or a combination of the two.

Feature capacity level

This setting controls the amount of memory reserved for downstream devices, timezone control, local linkages, and other features within the controller. A higher value reserves more room for these options while leaving less room for the cardholder database and event transaction buffer.

In the vast majority of circumstances, the default value of 3 should be left unchanged. This value will rarely need to be adjusted. If free memory in the panel becomes low, flagged by a “Panel Free Memory Low” Alarm, this value should be increased.

Values of less than 3 are not recommended. They can be used in the rare case when there are few downstream devices, few configured features, and maximum memory is required for the cardholder database and/or event transaction buffer.

Memory

Indicates the amount of memory that’s on the panel.

To enable biometric support, you must have 76 bytes of available memory. Additional memory is required to store templates on the panel. For more information, refer to the Biometrics Form on page 402 (non-segmented systems) or the Segments Form (Biometrics Sub-tab) on page 466 (segmented systems).

Badge IDs require 4 to 8 bytes of memory, depending on the number of digits in a badge. For more information, refer to the Hardware Settings Form on page 398 (non-segmented systems) or the Segments Form (Hardware Settings Sub-tab) on page 463 (segmented systems).

PIN type

Select the range of PIN digits allowed. Using PINs takes up memory on the access panel, which reduces the card capacity.

If you have a pin code configured for a controller that is 1-n digits long, but have a cardholder in the database that has a pin code longer than n, the pin code gets downloaded with the badge record, but gets truncated at n digits.

For example, you have a 1-4 digit pin for the controller, but the badge record in the access control system's database has '123456' specified as the pin code. When this gets downloaded, it is truncated to '1234.' The Cardholder can either enter the first 4 digits or all 6 digits correctly and gain access.

Cardholders

This field determines how much of the access panel's memory will be set aside for the cardholder records. This size is limited by the size of the access panel's memory, and is directly related to the options you choose in this section. The more options you choose and the more that each option requires (more digits in the card number, for example), the fewer the maximum number of cardholders possible.

Assets

Indicates the number of assets downloaded to the panels. To disable Asset Operations, set this value to 0.

Readers modules

Indicates the maximum number of reader devices that can be attached to this LNL-3300 access panel. The more reader modules you have attached, the fewer alarm panels can be attached. There is a fixed limit of 32 devices (modules + alarm panels), which cannot be adjusted.

Alarm panels

Indicates the maximum number of alarm panels that can be attached to this LNL-3300 access panel. There is a fixed limit of 32 devices (readers modules + alarm panels), which cannot be adjusted.

Store expiration date

If you want the badge expiration date to be used to determine the status of cards detected at the card readers, select "Date only" from the drop-down list. If the present date is later than the expiration date of the card, the card is considered to be invalid and access is denied.

If you do not want the badge expiration date to be used to determine the status of card, select "Not enforced" from the drop-down list.

A third option, "Date and time" is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge expiration date and time to be used to determine the status of cards detected at readers. If the present date and time is later than the expiration date and time of the card, the card is considered to be invalid and access is denied.

Store activation date

If you want the badge activation date to be used to determine the status of cards detected at the card readers, select "Date only" from the drop-down list. If the present date is earlier than the activation date of the card, the card is considered invalid and access is denied.

If you do not want the badge activation date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge activation date and time to be used to determine the status of cards detected at readers. If the present date and time is earlier than the activation date and time of the card, the card is considered to be invalid and access is denied.

Timed anti-passback

Indicates that readers attached to this panel are to be used for timed anti-passback. You must also set the **Timed anti-passback setting (minutes)** field. This is done on the Anti-Passback form of the Readers folder.

Store area anti-passback location

Select this check box if a reader attached to this access panel is used to enter or leave an anti-passback area. Anti-passback areas are defined on the Anti-Passback Areas form of the Areas folder. The **Area entering** and **Area leaving** fields, located on the Anti-Passback form of the Readers folder, are used to associate specific readers with specific areas.

Precision access (reader inclusion)

If selected, it indicates that this access panel will use the application’s precision access capabilities. Precision access is a method for assigning unique access privileges to individual cardholders. There is an infinite number of precision access combinations that can be created and assigned to cardholders.

Note: Using this option severely limits the number of cardholders that can be stored in the panel. If you wish to use precision access, it is recommended that panel memory be expanded to meet your facility’s needs.

Elevator support

If selected, this panel will support elevator control. You must have at least 1 MB of memory to use this feature. This check box will be grayed out if 256 KB of memory is used.

First card unlock

If selected, this panel will have first card unlock functionality.

First card unlock is used in conjunction with reader mode and timezone control. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.

Note: If the reader is in “Facility code only” mode, the first card unlock feature does not work.

HandKey biometrics

Enables hand geometry (HandKey) support. Specifically, this check box enables alternate readers to download templates to the panel.

76 bytes of memory are required to enable hand geometry support, and additional memory is required to store template information on the panel. For more information, refer to the System Options folder (non-segmented systems) or the Segments folder (segmented systems).

Note: The **Maximum templates** setting must be greater than zero (the default value) for the panel to support HandKey alternate readers. This setting is located on the System Options folder > Biometrics form (non-segmented systems) or the Segments form > Biometrics sub-tab (segmented systems).

Bioscrypt biometrics

Enables Bioscrypt alternate reader support. Specifically, this check box enables alternate readers to download templates to the panel.

76 bytes of memory are required to enable Bioscrypt biometric support, and additional memory is required to store template information on the access panel. For more information, refer to the System Options folder (non-segmented systems) or the Segments folder (segmented systems).

Note: The **Maximum templates** setting must be greater than zero (the default value) for the panel to support Bioscrypt alternate readers. This setting is located on the System Options folder > Biometrics form (non-segmented systems) or the Segments form > Biometrics sub-tab (segmented systems).

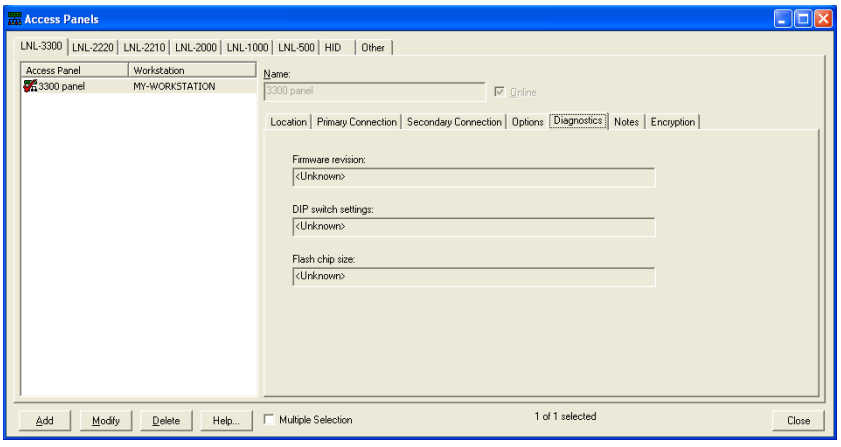
Special area rules

Checking this option enables the Special Two-Man Rule. If this is the first time enabling this rule a check will be made on your system and a message displayed informing you that additional changes may have to be made to the cardholder badge options. For more information please refer to Appendix G: Special Two-Man Rule on page 1435.

Event capacity

Fixed at 50,000. Unlike the other LNL- panels this does not change based on what options are selected.

LNL-3300 (Diagnostics Sub-tab)



Firmware revision

Displays the firmware revision reported by the controller the last time it was online. This is a read only text field.

DIP switch settings

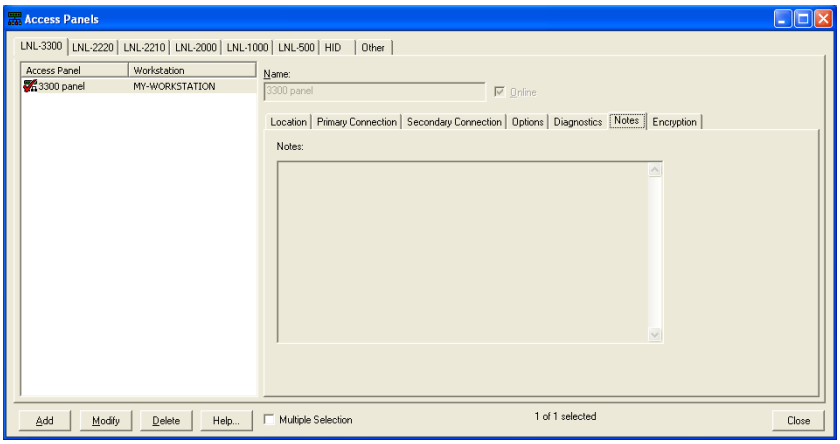
Displays the DIP switch settings reported by the controller, the last time it was online. This is a read only text field. Note that DIP switch settings are read by the controller only when the

controller is powered up. DIP switch changes made afterward will not take affect until the controller goes through another power cycle.

Flash chip size

Displays the flash chip size reported by the controller the last time it was online. This is a read only text field.

LNL-3300 (Notes Sub-tab)



Notes

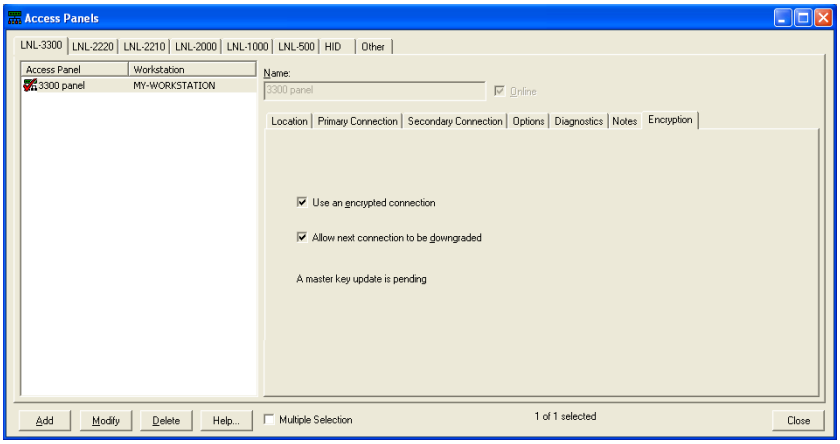
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

LNL-3300 (Encryption Sub-tab)

This view displays when the system/segment (the panel is associated with) uses automatic encryption. The same fields display when the system/segment is configured for manual encryption, except for the **Allow next connection to be downgraded** check box.The Encryption sub-tab does not display if a system/segment uses a plain connection.

Note: The system/segment the controller belongs to must be configured for encryption in order for this tab to display. The user must also have the correct user permissions.

For more information about encryption, refer to the Encryption for Controllers User Guide.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key, the factory default master keys, and finally by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible.

This check box displays only if the controller exists in an automatic key management system/segment.

A custom key update is pending

Indicates there is an outstanding key update for this controller. This is a read only field. This text field displays only if the controller exists in an automatic key management system/segment, and the condition exists (if there is an outstanding key update).

LNL-3300 Form Procedures

Add an LNL-3300 Access Panel

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu. Click the LNL-3300 tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the access panel.
4. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system or defining panels, but instead would wait until you're ready to put the panel into service.
5. Specify communication parameters on the Location, Primary Connection, and Secondary Connection sub-tabs.

6. Specify setup parameters on the Options sub-tab, which sets up the cardholder database for this panel.

   IMPORTANT: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

7. Click [OK].

Modify an LNL-3300 Access Panel

Notes: Modifying the PIN type requires a full panel download.

If the PIN type is modified on the controller and/or the General Cardholder Options form, you must log off/log on to System Administration before you modify a cardholder pin number.

1. In the listing window, select the LNL-3300 entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an LNL-3300 Access Panel

1. In the listing window, select the LNL-3300 entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enable an LNL-3300 Access Panel for Host Encryption

The encryption modify/export permission is required to complete this procedure.

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu.
2. On the LNL-3300 form, click the Encryption sub-tab.
3. In the listing window, select the LNL-3300 entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Enable an LNL-3300 Access Panel for Downstream Encryption

1. Download the latest firmware to all access panels, alarm panels, and readers.
2. Enable encryption on the system.
   a. Navigate to ***Administration > System Options*** or ***Administration > Segment Options*** if segmentation is enabled.

b. Click [Modify].
c. On the Controller Encryption tab, select either Manual key management encryption or Automatic key management encryption from the **Connection type** drop-down.
d. Click [OK].

3. Enable host and downstream encryption.
   a. Navigate to ***Access control*** > ***Access Panels***.
   b. On the LNL-3300 form, select the Encryption sub-tab.
   c. In the Access Panel listing window select an access panel you wish to configure downstream encryption for.
   d. Select the **Use an encrypted connection** check box.
   e. Select the **Allow downstream encryption** check box.
   f. To add a downstream encryption key, click [Add Master Key]. The Master Key Entry window opens. Select the options appropriate for your system.
4. Set the encryption level for each reader that needs to be encrypted. For more information, refer to General Form on page 635.
   a. Navigate to ***Access Control*** > ***Readers***.
   b. On the Reader tab, select the readers to be encrypted in the Reader listing window. Click [Modify].
   c. Select the encryption level from the **Encrypted Communications Mode** drop-down box. If Encrypted Communications Mode is set to “Custom” then first download the master keys as described in step 6 before completing this step.
5. Set the encryption level for each alarm panel that needs to be encrypted. For more information, refer to Alarm Panels Form on page 685.
   a. Navigate to ***Access Control*** > ***Alarm Panels***. Only LNL-1100 and LNL-1200 alarm panels can be configured for downstream encryption.
   b. On the Alarm Panels tab, select the panels to be encrypted in the Alarm Panel listing window. Click [Modify].
   c. Select the encryption level from the **Encrypted Communications Mode** drop-down box. If Encrypted Communications Mode is set to “Custom” then first download the master keys as described in step 6 before completing this step.
6. In the Alarm Monitoring application, download the master keys to the access panels and other devices.
   a. In the hardware tree, right-click the access panel and select “Download encryption keys.”
   b. Verify that the connection is encrypted as requested by looking at each devices encryption status in the alarm monitoring hardware tree.

Enter Notes for an Access Panel

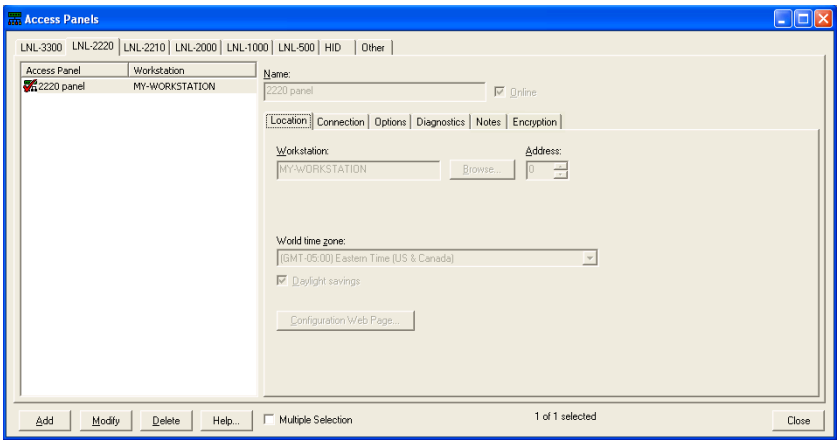
1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

LNL-2220 Form Overview

This form is used to:

- Assign names to individual LNL-2220 type access panels in the software
- Specify access panel setup parameters, including information stored in the panel
- Specify communication panel setup parameters, including the workstation associated with the panel and the access method (direct serial connection, LAN, or dialup)
- View the firmware, DIP switch settings and flash chip size of the panel
- Enable encryption, if you have the proper user permission

LNL-2220 Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the access panel. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Selects the workstation or server to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

Address

Specifies the panel's address, which must match the DIP switch setting on the panel itself. Possible values are in the range of 0 through 7. The factory default DIP switch setting is 0.

For any panel(s) that will be communicating with a workstation using a dialup connection, the panel(s) must be set to address 1 or the dial-back to host capability will fail.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Configuration Web Page

Opens the web page used to configure the access panel. Only available when in view mode and if the controller has an IP address or host name configured for the primary connection.

Add

Adds a panel entry.

Modify

Changes a panel entry.

Delete

Removes a panel entry.

Help

Displays online help for this topic.

Change Segment

Displays if segmentation is enabled and you are in modify mode. Click this button to move the access panel to a different segment.

Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected panels.

Mode

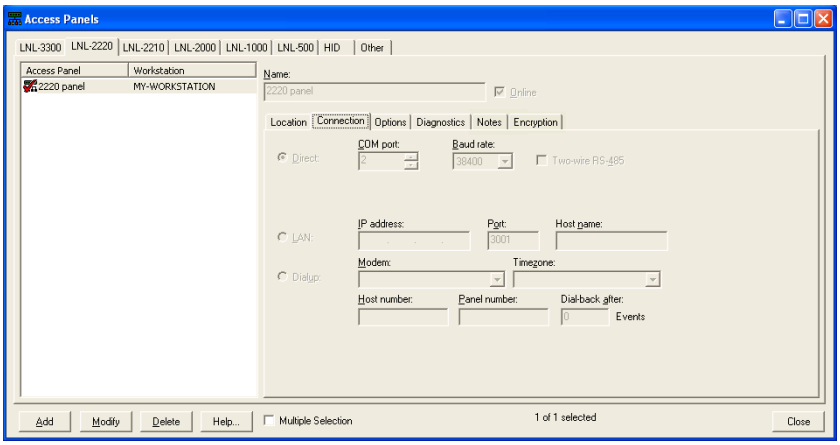
In view mode, indicates how many panels are currently selected, and the current total number of panels; for example, "2 of 5 selected".

In modify mode, indicates the current operation (Add Mode, Modify Mode, etc.).

Close

Closes the Access Panels folder.

LNL-2220 Form (Connection Sub-tab)



Direct

Select this radio button if communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**, the **Baud rate**, and whether or not communication to the host will use a **Two-wire RS-485** connection.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 through 255.

Baud rate

If you selected the **Direct** radio button, this is the speed (in bits per second) at which information is transferred between the workstation and the access panel via the serial connection.

Note: Some third party devices do not allow the baud rate to be modified from the host application software. If such a device is in use, the baud rate setting in OnGuard has no bearing. Refer to the documentation for any third party devices being used.

Two-wire RS-485

Other panels can be configured to communicate with the host workstation using either a 4-wire or 2-wire RS-485 connection. Select this check box if 2-wire communication is to be used.

LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's IP address.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Port

The network port that the LAN connection will be established on. This needs to match what is specified in the LNL-2220 configuration web page. The default is 3001.

Host name

The host name that the LNL-2220 will use with DHCP and will register with the DHCP server. Instead of referencing the panel by a static IP address you may be able to reference it by the host name depending on your network configuration.

Dialup

Select this radio button if the workstation will communicate with the access panel using a dialup connection. This option functions together with the LAN option on the Secondary Connection sub-tab to limit combinations of primary and secondary communications for dual path usage.

You must also specify the workstation's modem, timezone, host number, panel number and dial-back after__events.

Modem

If you selected the **Dialup** radio button, select the modem on the workstation that will be used for dialup communication with the access panel. Choices include all TAPI (Telephone Application Programming Interface) devices that are currently configured on the specified Workstation.

Before a modem can be listed in this drop-down list, the modem must be properly configured for the selected workstation. This is done on the Modems form in the Dialup Configuration folder, which is reached by selecting ***Modems*** from the ***Access Control*** menu. For more information, refer to Connect a Modem to a Lenel Access Panel on page 704.

If any of the TAPI devices are used for other dial functions such as remote access, do not select them for panel dial usage.

For more information, refer to your Windows user guide.

Timezone

If you selected the **Dialup** radio button, indicate the timezone during which the access panel will initiate dialup communication with the workstation. You can select only one timezone for the particular workstation-modem-panel combination. Timezones are defined on the Timezones form of the Timezones folder.

Functionally, at the start of each interval that comprises the timezone, the panel will automatically dial the host number. If a connection cannot be established, it will redial until a connection can be made. Once connected, all transactions stored in the panel will be dumped to the Communication Server (on the workstation) to be logged in the database. In addition, all commands that need to be sent to the panel will be sent from the host at that time.

Timezone (continued)

After all information is transferred, the Communication Server will automatically terminate the dialup connection with the panel. The exception to this occurs if you select the "Always" timezone. In that situation, the workstation will attempt to always stay connected to the panel via dial-up. Functionally, this is similar to communicating with the workstation via a direct (serial) or LAN connection.

Multiple workstations can use the same TAPI modem, or one workstation might have access to multiple TAPI modems. However, only one connection to a particular modem can be established at a particular time. For example, a particular workstation might use a particular modem to dial one panel at 12:00, a second panel at 1:00, a third panel at 2:00, etc.

Host number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the workstation. This is the number that the access panel will use to dial into the panel to send events and other transactions to the workstation.

Type the exact dialing sequence here. Although you can use parentheses and dashes, they are ignored by TAPI devices. For example, 2489720 and (212) 546-1234. For more information, refer to your Windows user guide.

Panel number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the access panel. This is the number that the workstation would need to dial to communicate with the access panel.

Typically, all communication between the access panel and the workstation is initiated from the panel. However, the workstation can dial the panel from within the Alarm Monitoring system. This is done by right-clicking on the panel's entry in the System Tree, then selecting the **Connect** command from the popup menu.

Any ASCII string can be typed here (for example, a comma typically triggers a pause in the dialing sequence).

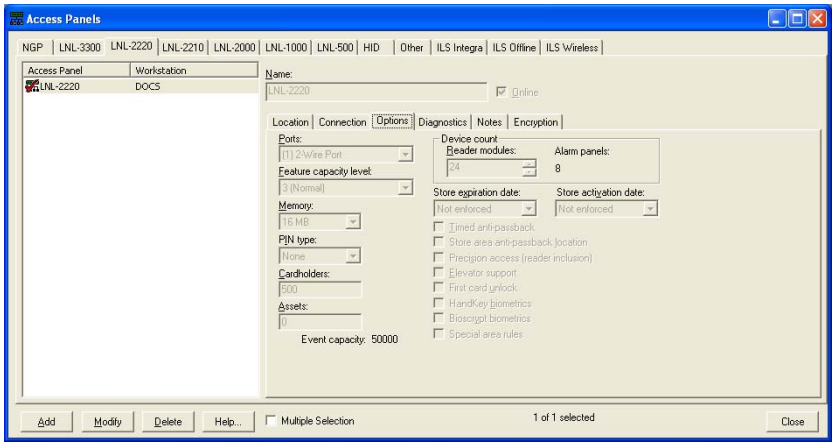
Dial-back after__Events

This field is displayed only if you have selected the **Dialup** radio button. LNL-2220 panels can be programmed to dial the workstation after a certain number of events have been stored in the panel but have not yet been reported to the host (because the panel has been offline).

When the panel has accumulated the specified number of stored events, the panel will automatically dial the host number to dump its transactions and to receive any command programming. After the information has been exchanged, the workstation will terminate the connection.

The default value here is 255 events. The minimum value you can enter is zero (meaning that the panel will never dial the host). The maximum value is equal to one less than the maximum number of events that the panel can store.

LNL-2220 (Options Sub-tab)



Note: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been

added. Changing these settings will result in a full cardholder database download to the panel.

Ports

Access panels communicate with its downstream devices (reader interfaces, input control modules, and output control modules) using either 2- or 4-wire RS-485 communication, or a combination of the two.

Feature capacity level

This setting controls the amount of memory reserved for downstream devices, timezone control, local linkages, and other features within the controller. A higher value reserves more room for these options while leaving less room for the cardholder database and event transaction buffer.

In the vast majority of circumstances, the default value of 3 should be left unchanged. This value will rarely need to be adjusted. If free memory in the panel becomes low, flagged by a “Panel Free Memory Low” Alarm, this value should be increased.

Values of less than 3 are not recommended. They can be used in the rare case when there are few downstream devices, few configured features, and maximum memory is required for the cardholder database and/or event transaction buffer.

Memory

Indicates the amount of memory that’s on the panel.

To enable biometric support, you must have 76 bytes of available memory. Additional memory is required to store templates on the panel. For more information, refer to the Biometrics Form on page 402 (non-segmented systems) or the Segments Form (Biometrics Sub-tab) on page 466 (segmented systems).

Badge IDs require 4 to 8 bytes of memory, depending on the number of digits in a badge. For more information, refer to the Hardware Settings Form on page 398 (non-segmented systems) or the Segments Form (Hardware Settings Sub-tab) on page 463 (segmented systems).

PIN type

Select the range of PIN digits allowed. Using PINs takes up memory on the access panel, which reduces the card capacity.

If you have a pin code configured for a controller that is 1-n digits long, but have a cardholder in the database that has a pin code longer than n, the pin code gets downloaded with the badge record, but gets truncated at n digits. For example, you have a 1-4 digit pin for the controller, but the badge record in the access control system’s database has ‘123456’ specified as the pin code. When this gets downloaded, it is truncated to ‘1234.’ The Cardholder can either enter the first 4 digits or all 6 digits correctly and gain access.

Cardholders

This field determines how much of the access panel’s memory will be set aside for the cardholder records. This size is limited by the size of the access panel’s memory, and is directly related to the options you choose in this section. The more options you choose and the more that each option requires (more digits in the card number, for example), the fewer the maximum number of cardholders possible.

Assets

Indicates the number of assets downloaded to the panels. To disable Asset Operations, set this value to 0.

Readers modules

Select the number of reader modules you plan to attach to this LNL-2220 access panel. The more reader devices you have attached, the fewer alarm panels can be attached.

The actual number of readers devices that can be attached to the access panel is directly related to both the number of reader devices that are configured AND to the type of reader device(s) installed. Two readers can be attached to a Dual-Reader Interface board. One reader can be attached to a Single Reader Interface board.

You can choose a value in the range of 16 through 32. The value in the **Alarm panels** field is adjusted accordingly. For the LNL-2220, the total number of devices (reader modules + alarm panels) cannot exceed 32.

Alarm panels

Indicates the maximum number of alarm panels that can be attached to this LNL-2220 access panel. You can change this field only indirectly, by modifying the **Readers modules** field on this form. The more readers you have attached, the fewer alarm panels can be attached.

Store expiration date

If you want the badge expiration date to be used to determine the status of cards detected at the card readers, select “Date only” from the drop-down list. If the present date is later than the expiration date of the card, the card is considered to be invalid and access is denied.

If you do not want the badge expiration date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge expiration date and time to be used to determine the status of cards detected at readers. If the present date and time is later than the expiration date and time of the card, the card is considered to be invalid and access is denied.

Store activation date

If you want the badge activation date to be used to determine the status of cards detected at the card readers, select “Date only” from the drop-down list. If the present date is earlier than the activation date of the card, the card is considered invalid and access is denied.

If you do not want the badge activation date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge activation date and time to be used to determine the status of cards detected at readers. If the present date and time is earlier than the activation date and time of the card, the card is considered to be invalid and access is denied.

Timed anti-passback

Indicates that readers attached to this panel are to be used for timed anti-passback. You must also set the **Timed anti-passback setting (minutes)** field. This is done on the Anti-Passback form of the Readers folder.

Store area anti-passback location

Select this check box if a reader attached to this access panel is used to enter or leave an anti-passback area. Anti-passback areas are defined on the Anti-Passback Areas form of the Areas folder. The **Area entering** and **Area leaving** fields, located on the Anti-Passback form of the Readers folder, are used to associate specific readers with specific areas.

Precision access (reader inclusion)

If selected, it indicates that this access panel will use the application's precision access capabilities. Precision access is a method for assigning unique access privileges to individual cardholders. There is an infinite number of precision access combinations that can be created and assigned to cardholders.

Note: Using this option severely limits the number of cardholders that can be stored in the panel. If you wish to use precision access, it is recommended that panel memory be expanded to meet your facility's needs.

Elevator support

If selected, this panel will support elevator control. You must have at least 1 MB of memory to use this feature. This check box will be grayed out if 256 KB of memory is used.

First card unlock

If selected, this panel will have first card unlock functionality.

First card unlock is used in conjunction with reader mode and timezone control. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like "snow days" when employees can't make it to work on time.

Note: If the reader is in "Facility code only" mode, the first card unlock feature does not work.

HandKey biometrics

Enables hand geometry (HandKey) support. Specifically, this check box enables alternate readers to download templates to the panel.

76 bytes of memory are required to enable hand geometry support, and additional memory is required to store template information on the panel. For more information, refer to the System Options folder (non-segmented systems) or the Segments folder (segmented systems).

Note: The **Maximum templates** setting must be greater than zero (the default value) for the panel to support HandKey alternate readers. This setting is located on the System Options folder > Biometrics form (non-segmented systems) or the Segments form > Biometrics sub-tab (segmented systems).

Bioscrypt biometrics

Enables Bioscrypt alternate reader support. Specifically, this check box enables alternate readers to download templates to the panel.

76 bytes of memory are required to enable Bioscrypt biometric support, and additional memory is required to store template information on the access panel. For more information, refer to the System Options folder (non-segmented systems) or the Segments folder (segmented systems).

Note: The **Maximum templates** setting must be greater than zero (the default value) for the panel to support Bioscrypt alternate readers. This setting is located on the System Options folder > Biometrics form (non-segmented systems) or the Segments form > Biometrics sub-tab (segmented systems).

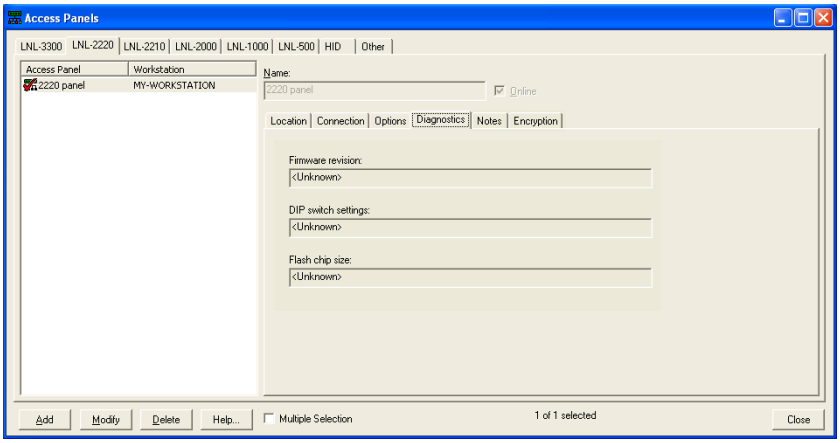
Special area rules

Checking this option enables the Special Two-Man Rule. If this is the first time enabling this rule a check will be made on your system and a message displayed informing you that additional changes may have to be made to the cardholder badge options. For more information please refer to Appendix G: Special Two-Man Rule on page 1435.

Event capacity

Fixed at 50,000. Unlike the other LNL- panels this does not change based on what options are selected.

LNL-2220 (Diagnostics Sub-tab)



Firmware revision

Displays the firmware revision reported by the controller the last time it was online. This is a read only text field.

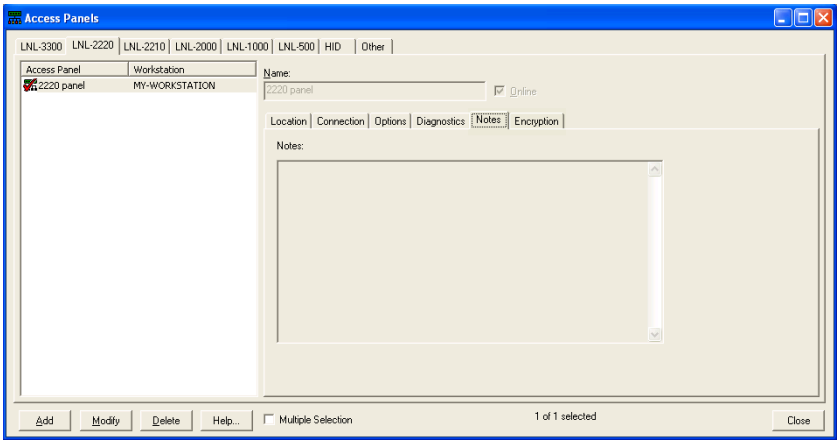
DIP switch settings

Displays the DIP switch settings reported by the controller, the last time it was online. This is a read only text field. Note that DIP switch settings are read by the controller only when the controller is powered up. DIP switch changes made afterward will not take affect until the controller goes through another power cycle.

Flash chip size

Displays the flash chip size reported by the controller the last time it was online. This is a read only text field.

LNL-2220 (Notes Sub-tab)



Notes

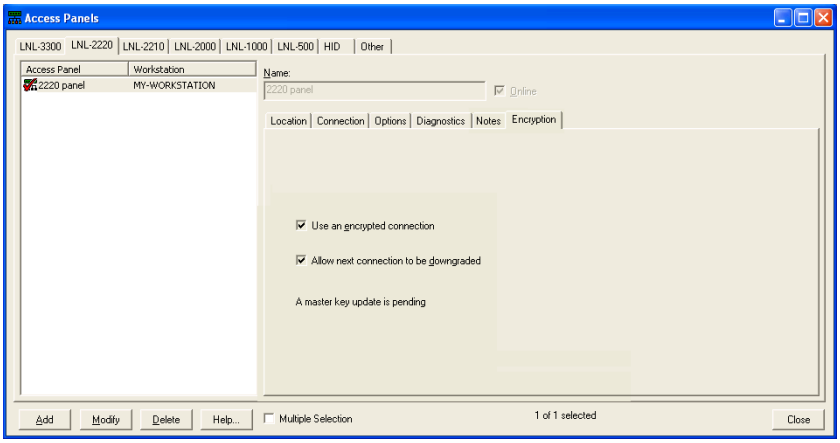
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

LNL-2220 (Encryption Sub-tab)

This view displays when the system/segment (the panel is associated with) uses automatic encryption. The same fields display when the system/segment is configured for manual encryption, except for the **Allow next connection to be downgraded** check box.The Encryption sub-tab does not display if a system/segment uses a plain connection.

Note: The system/segment the controller belongs to must be configured for encryption in order for this tab to display. The user must also have the correct user permissions.

For more information about encryption, refer to the Encryption for Controllers User Guide.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key, the factory default master keys, and finally by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible.

This check box displays only if the controller exists in an automatic key management system/ segment.

A custom key update is pending

Indicates there is an outstanding key update for this controller. This is a read only field.

This text field displays only if the controller exists in an automatic key management system/ segment, and the condition exists (if there is an outstanding key update).

LNL-2220 Form Procedures

Add an LNL-2220 Access Panel

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu. Click the LNL-2220 tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the access panel.
4. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system or defining panels, but instead would wait until you're ready to put the panel into service.
5. Specify communication parameters on the Location, Primary Connection, and Secondary Connection sub-tabs.
6. Specify setup parameters on the Options sub-tab, which sets up the cardholder database for this panel.

   IMPORTANT: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

7. Click [OK].

Modify an LNL-2220 Access Panel

Notes: Modifying the PIN type requires a full panel download.

If the PIN type is modified on the controller and/or the General Cardholder Options form, you must log off/log on to System Administration before you modify a cardholder pin number.

1. In the listing window, select the LNL-2220 entry you wish to change.

2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an LNL-2220 Access Panel

1. In the listing window, select the LNL-2220 entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enable an LNL-2220 Access Panel for Encryption

The encryption modify/export permission is required to complete this procedure.

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu.
2. On the LNL-2220 form, click the Encryption sub-tab.
3. In the listing window, select the LNL-2220 entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Enable an LNL-2220 Access Panel for Downstream Encryption

1. Download the latest firmware to all access panels, alarm panels, and readers.
2. Enable encryption on the system.
   a. Navigate to ***Administration*** > ***System Options*** or ***Administration*** > ***Segment Options*** if segmentation is enabled.
   b. Click [Modify].
   c. On the Controller Encryption tab, select either Manual key management encryption or Automatic key management encryption from the **Connection type** drop-down box.
   d. Click [OK].
3. Enable host and downstream encryption.
   a. Navigate to ***Access control*** > ***Access Panels***.
   b. On the LNL-2220 form, select the Encryption sub-tab.
   c. In the Access Panel listing window select an access panel you wish to configure downstream encryption for.
   d. Select the **Use an encrypted connection** check box.
   e. Select the **Allow downstream encryption** check box.
   f. To add a downstream encryption key, click [Add Master Key]. The Master Key Entry window opens. Select the options appropriate for your system.
4. Set the encryption level for each reader that needs to be encrypted. For more information, refer to General Form on page 635.
   a. Navigate to ***Access Control*** > ***Readers***.

b. On the Reader tab, select the readers to be encrypted in the Reader listing window. Click [Modify].

c. Select the encryption level from the **Encrypted Communications Mode** drop-down box. If Encrypted Communications Mode is set to "Custom" then first download the master keys as described in step 6 before completing this step.

5. Set the encryption level for each alarm panel that needs to be encrypted. For more information, refer to Alarm Panels Form on page 685.

a. Navigate to ***Access Control*** > ***Alarm Panels***. Only LNL-1100 and LNL-1200 alarm panels can be configured for downstream encryption.

b. On the Alarm Panels tab, select the panels to be encrypted in the Alarm Panel listing window. Click [Modify].

c. Select the encryption level from the **Encrypted Communications Mode** drop-down box. If Encrypted Communications Mode is set to "Custom" then first download the master keys as described in step 6 before completing this step.

6. In the Alarm Monitoring application, download the master keys to the access panels and other devices.

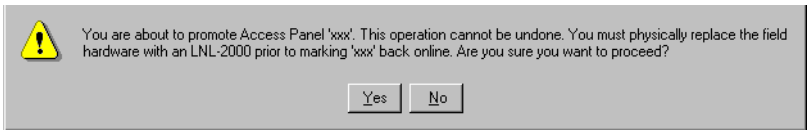
a. In the hardware tree, right-click the access panel and select "Download encryption keys."

b. Verify that the connection is encrypted as requested by looking at each devices encryption status in the alarm monitoring hardware tree.

Promote an LNL-2220 Access Panel to an LNL-3300

Note: In order to promote an access panel, it must be offline.

1. In the listing window, right-click over the LNL-2220 entry you wish to promote.
2. From the pop-up menu, select **Promote Access Panel to LNL-3300**. The following message will be displayed:



3. Click [Yes] to continue.
4. Click [OK].

Enter Notes for an Access Panel

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

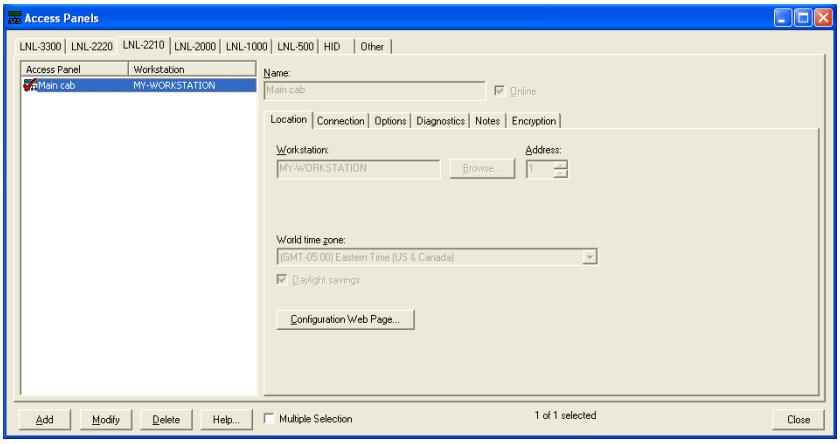
LNL-2210 Form Overview

This form is used to:

- Assign names to individual LNL-2210 type access panels in the software

- Specify access panel setup parameters, including information stored in the panel
- Specify communication panel setup parameters, including the workstation associated with the panel and the access method
- View the firmware, DIP switch settings and flash chip size of the panel
- Enable encryption, if you have the proper user permission

LNL-2210 Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the access panel. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Selects the workstation or server to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Note: You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

Address

Specifies the panel's address, which must match the DIP switch setting on the panel itself. Possible values are in the range of 0 through 7. The factory default DIP switch setting is 0.

Note: For any panel(s) that will be communicating with a workstation using a dialup connection, the panel(s) must be set to address 1 or the dial-back to host capability will fail.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Configuration Web Page

Opens the web page used to configure the access panel. Only available when in view mode and if the controller has an IP address or host name configured for the primary connection.

Add

Adds a panel entry.

Modify

Changes a panel entry.

Delete

Removes a panel entry.

Help

Displays online help for this topic.

Change Segment

Displays if segmentation is enabled and you are in modify mode. Click this button to move the access panel to a different segment.

Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected panels.

Mode

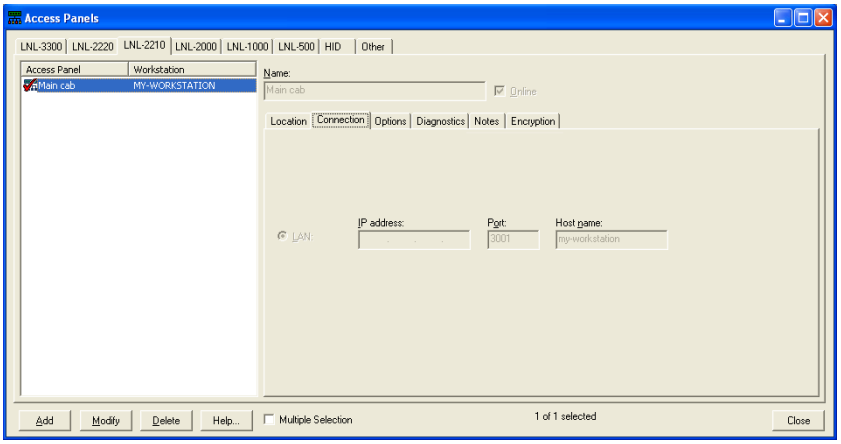
In view mode, indicates how many panels are currently selected, and the current total number of panels; for example, "2 of 5 selected".

In modify mode, indicates the current operation (Add Mode, Modify Mode, etc.).

Close

Closes the Access Panels folder.

LNL-2210 Form (Connection Sub-tab)



LAN

The workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's IP address or host name.

IP address

Enter the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

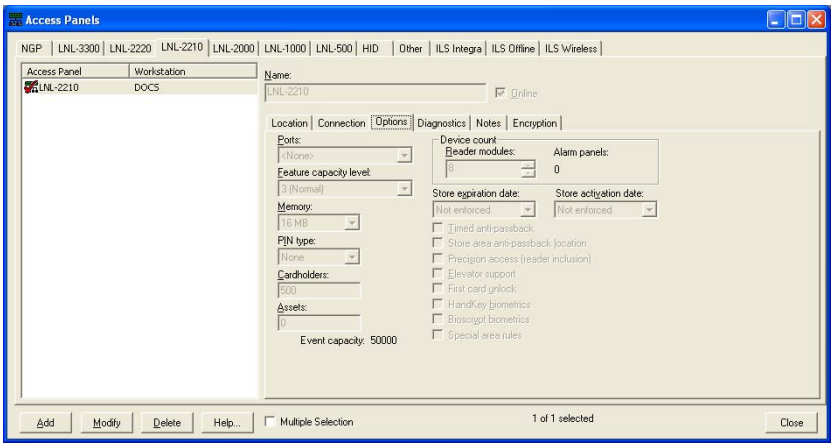
Port

The network port that the LAN connection will be established on. This needs to match what is specified in the LNL-2210 configuration web page. The default is 3001.

Host name

The host name that the LNL-2210 will use with DHCP and will register with the DHCP server. Instead of referencing the panel by a static IP address you may be able to reference it by the host name depending on your network configuration.

LNL-2210 (Options Sub-tab)



Note: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

Ports

This access panels does not support downstream devices (reader interfaces, input control modules, and output control modules); therefore, this field is disabled.

Feature capacity level

This field is disabled.

Memory

This field is disabled.

PIN type

Select the range of PIN digits allowed. Using PINs takes up memory on the access panel, which reduces the card capacity.

If you have a PIN code configured for a controller that is 1-n digits long, but have a cardholder in the database that has a pin code longer than n, the pin code gets downloaded with the badge record, but gets truncated at n digits.

For example, you have a 1-4 digit pin for the controller, but the badge record in the access control system's database has '123456' specified as the pin code. When this gets downloaded, it is truncated to '1234.' The Cardholder can either enter the first 4 digits or all 6 digits correctly and gain access.

Cardholders

This field determines how much of the access panel's memory will be set aside for the cardholder records. This size is limited by the size of the access panel's memory, and is directly related to the options you choose in this section. The more options you choose and the more that each option requires (more digits in the card number, for example), the fewer the maximum number of cardholders possible.

Assets

Indicates the number of assets downloaded to the panels. To disable Asset Operations, set this value to 0.

Readers modules

Indicates the maximum number of reader devices that can be attached to this LNL-2210 access panel. The more reader modules you have attached, the fewer alarm panels can be attached. There is a fixed limit of 8 devices (reader modules + alarm panels) which cannot be adjusted.

Select the number of reader modules you plan to attach to this LNL-2210 access panel. The more reader devices you have attached, the fewer alarm panels can be attached.

The actual number of readers devices that can be attached to the access panel is directly related to both the number of reader devices configured AND to the type of reader devices installed. Two readers can be attached to a Dual-Reader Interface board. One reader can be attached to a Single Reader Interface board.

You can choose a value from 0 - 8. The value in the **Alarm panels** field is adjusted accordingly. For the LNL-2210, the total number of devices (reader modules + alarm panels) cannot exceed 8.

Alarm panels

Indicates the maximum number of alarm panels that can be attached to this LNL-2210 access panel. There is a fixed limit of 8 devices (readers modules + alarm panels) which cannot be adjusted.

You can change this field only indirectly by modifying the **Readers modules** field on this form. The more readers you have attached, the fewer alarm panels can be attached.

Store expiration date

If you want the badge expiration date to be used to determine the status of cards detected at the card readers, select “Date only” from the drop-down list. If the present date is later than the expiration date of the card, the card is considered to be invalid and access is denied.

If you do not want the badge expiration date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge expiration date and time to be used to determine the status of cards detected at readers. If the present date and time is later than the expiration date and time of the card, the card is considered to be invalid and access is denied.

Store activation date

If you want the badge activation date to be used to determine the status of cards detected at the card readers, select “Date only” from the drop-down list. If the present date is earlier than the activation date of the card, the card is considered invalid and access is denied.

If you do not want the badge activation date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge activation date and time to be used to determine the status of cards detected at readers. If the present date and time is earlier than the activation date and time of the card, the card is considered to be invalid and access is denied.

Timed anti-passback

Indicates that readers attached to this panel are to be used for timed anti-passback. You must also set the **Timed anti-passback setting (minutes)** field. This is done on the Anti-Passback form of the Readers folder.

Store area anti-passback location

Select this check box if a reader attached to this access panel is used to enter or leave an anti-passback area. Anti-passback areas are defined on the Anti-Passback Areas form of the Areas folder. The **Area entering** and **Area leaving** fields, located on the Anti-Passback form of the Readers folder, are used to associate specific readers with specific areas.

Precision access (reader inclusion)

If selected, it indicates that this access panel will use the application's precision access capabilities. Precision access is a method for assigning unique access privileges to individual cardholders. There is an infinite number of precision access combinations that can be created and assigned to cardholders.

Note: Using this option severely limits the number of cardholders that can be stored in the panel. If you wish to use precision access, it is recommended that panel memory be expanded to meet your facility's needs.

Elevator support

If selected, this panel will support elevator control. You must have at least 1 MB of memory to use this feature. This check box will be grayed out if 256 KB of memory is used.

Note: Depending on the number of elevator floors supported, you may need to modify the default device count of 8 reader modules and 0 alarm panels. This is not required for a 6-floor elevator, but for the other Lenel elevator solutions, the number of alarm panels must be increased by 1 for each set of 16 floors supported unless floor tracking is enabled. If floor tracking is enabled, the number of alarm panels must be increased by 2 for each set of 16 floors. For example, 1 - 16 floors (with floor tracking) require at least 2 alarm panels; 17 - 32 floors (with floor tracking) require at least 4 alarm panels.

First card unlock

If selected, this panel will have first card unlock functionality. First card unlock is used in conjunction with reader mode and timezone control. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like "snow days" when employees can't make it to work on time.

Note: If the reader is in "Facility code only" mode, the first card unlock feature does not work.

HandKey biometrics

Enables hand geometry (HandKey) support. Specifically, this check box enables alternate readers to download templates to the panel.

76 bytes of memory are required to enable hand geometry support, and additional memory is required to store template information on the panel. For more information, refer to the System Options folder (non-segmented systems) or the Segments folder (segmented systems).

The Maximum templates setting must be greater than zero (the default value) for the panel to support HandKey alternate readers. This setting is located on the System Options folder >

Biometrics form (non-segmented systems) or the Segments form > Biometrics sub-tab (segmented systems).

Bioscrypt biometrics

Enables Bioscrypt alternate reader support. Specifically, this check box enables alternate readers to download templates to the panel.

76 bytes of memory are required to enable Bioscrypt biometric support, and additional memory is required to store template information on the access panel. For more information, refer to the System Options folder (non-segmented systems) or the Segments folder (segmented systems).

Note: The **Maximum templates** setting must be greater than zero (the default value) for the panel to support Bioscrypt alternate readers. This setting is located on the System Options folder > Biometrics form (non-segmented systems) or the Segments form > Biometrics sub-tab (segmented systems).

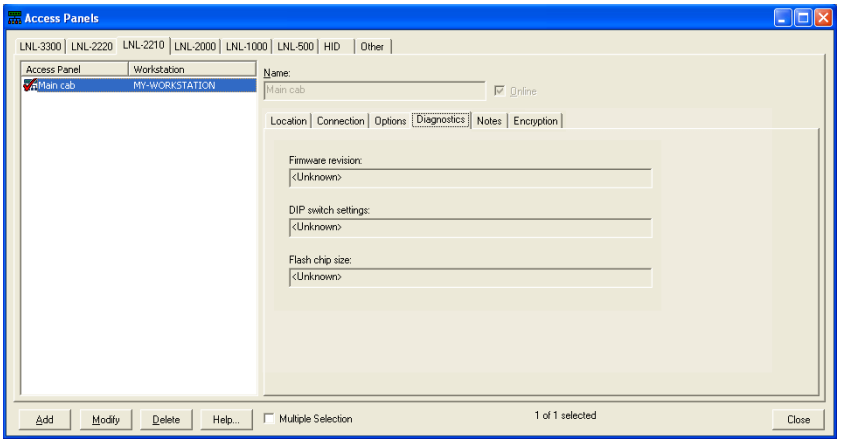
Special area rules

Checking this option enables the Special Two-Man Rule. If this is the first time enabling this rule a check will be made on your system and a message displayed informing you that additional changes may have to be made to the cardholder badge options. For more information please refer to Appendix G: Special Two-Man Rule on page 1435.

Event capacity

Fixed at 50,000. Unlike the other panels, this does not change based on what options are selected.

LNL-2210 (Diagnostics Sub-tab)



Firmware revision

Displays the firmware revision reported by the controller the last time it was online. This is a read only text field.

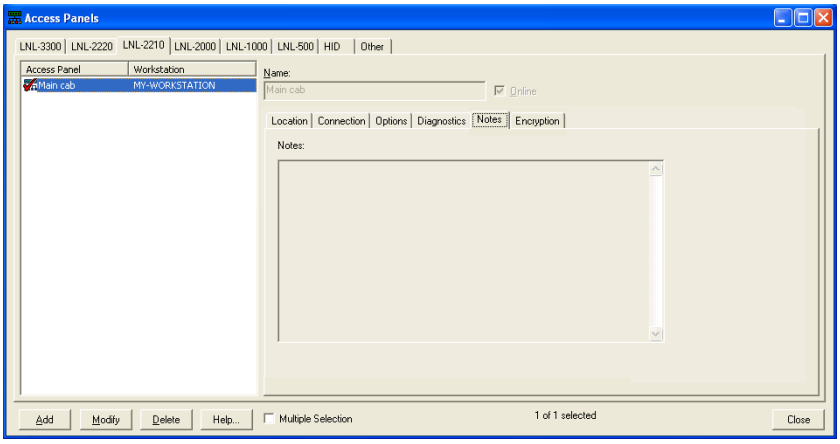
DIP switch settings

Displays the DIP switch settings reported by the controller, the last time it was online. This is a read only text field. Note that DIP switch settings are read by the controller only when the controller is powered up. DIP switch changes made afterward will not take affect until the controller goes through another power cycle.

Flash chip size

Displays the flash chip size reported by the controller the last time it was online. This is a read only text field.

LNL-2210 (Notes Sub-tab)



Notes

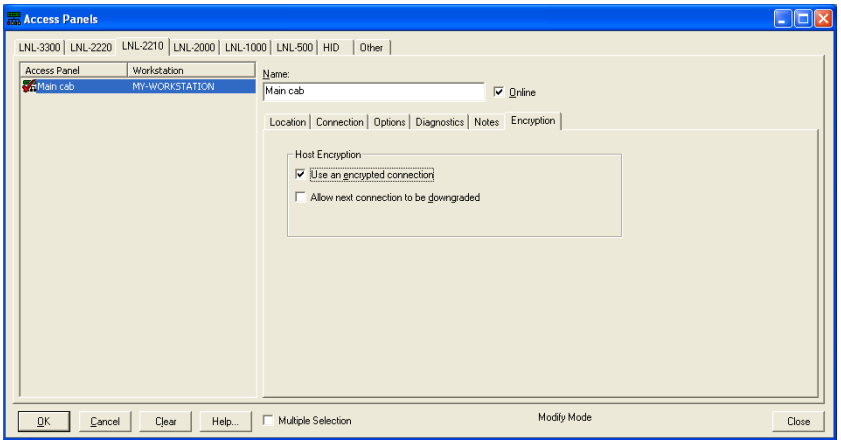
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

LNL-2210 (Encryption Sub-tab)

This view displays when the system/segment (the panel is associated with) uses automatic encryption. The same fields display when the system/segment is configured for manual encryption, except for the **Allow next connection to be downgraded** check box.The Encryption sub-tab does not display if a system/segment uses a plain connection.

Note: The system/segment the controller belongs to must be configured for encryption in order for this tab to display. The user must also have the correct user permissions.

For more information about encryption, refer to the Encryption for Controllers User Guide.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key, the factory default master keys, and finally by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible.

This check box displays only if the controller exists in an automatic key management system/segment.

A custom key update is pending

Indicates there is an outstanding key update for this controller. This is a read only field. This text field displays only if the controller exists in an automatic key management system/segment, and the condition exists (if there is an outstanding key update).

LNL-2210 Form Procedures

Add an LNL-2210 Access Panel

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu. Click the LNL-2210 tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the access panel.
4. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system or defining panels, but instead would wait until you're ready to put the panel into service.
5. Specify communication parameters on the Location and Connection sub-tabs.

6. Specify setup parameters on the Options sub-tab, which sets up the cardholder database for this panel.

   IMPORTANT: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

7. Click [OK].

Modify an LNL-2210 Access Panel

Notes: Modifying the PIN type requires a full panel download.

If the PIN type is modified on the controller and/or the General Cardholder Options form, you must log off/log on to System Administration before you modify a cardholder pin number.

1. In the listing window, select the LNL-2210 entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an LNL-2210 Access Panel

1. In the listing window, select the LNL-2210 entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enable an LNL-2210 Access Panel for Encryption

The encryption modify/export permission is required to complete this procedure.

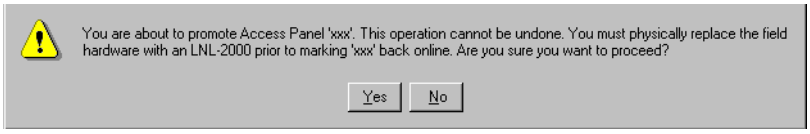
1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu.
2. On the LNL-2210 form, click the Encryption sub-tab.
3. In the listing window, select the LNL-2210 entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Promote an LNL-2210 Access Panel to anLNL-2220 or LNL-3300

Note: In order to promote an access panel, it must be offline.

1. In the listing window, right-click over the LNL-2210 entry you wish to promote.

2. From the pop-up menu, select **Promote Access Panel to LNL-2200** or **Promote Access Panel to LNL-3300**. The following message will be displayed:



3. Click [Yes] to continue.
4. Click [OK].

Enter Notes for an Access Panel

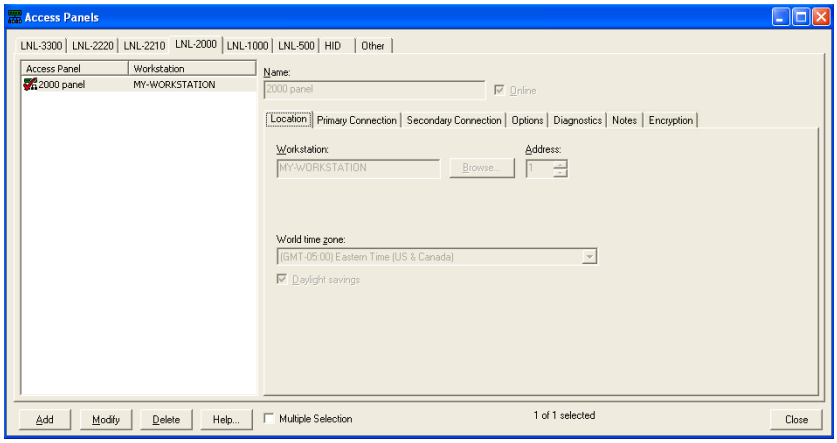
1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

LNL-2000 Form Overview

This form is used to:

- Assign names to individual LNL-2000 type access panels in the software
- Specify access panel setup parameters, including information stored in the panel
- Specify communication panel setup parameters, including the workstation associated with the panel and the access method (direct serial connection, LAN, or dialup)
- View the firmware, DIP switch settings and flash chip size of the panel
- Enable encryption, if you have the proper user permission

LNL-2000 Form (Location Sub-tab)



Listing window
Lists currently defined access panels and the name of the workstation that is connected to each.

Name
Enter a name for the access panel. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online
If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation
Selects the workstation or server to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Note: You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse
Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

Address
Specifies the panel’s address, which must match the DIP switch setting on the panel itself. Possible values are in the range of 0 through 7. The factory default DIP switch setting is 0.

For any panel(s) that will be communicating with a workstation using a dialup connection, the panel(s) must be set to address 1 or the dial-back to host capability will fail.

World time zone
Select the world time zone for the selected access panel’s geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone’s clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings
Select this check box if Daylight Savings Time is enforced in the selected access panel’s geographical location.

Add
Adds a panel entry.

Modify
Changes a panel entry.

Delete
Removes a panel entry.

Help
Displays online help for this topic.

Change Segment
Displays if segmentation is enabled and you are in modify mode. Click this button to move the access panel to a different segment.

Multiple Selection
If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected panels.

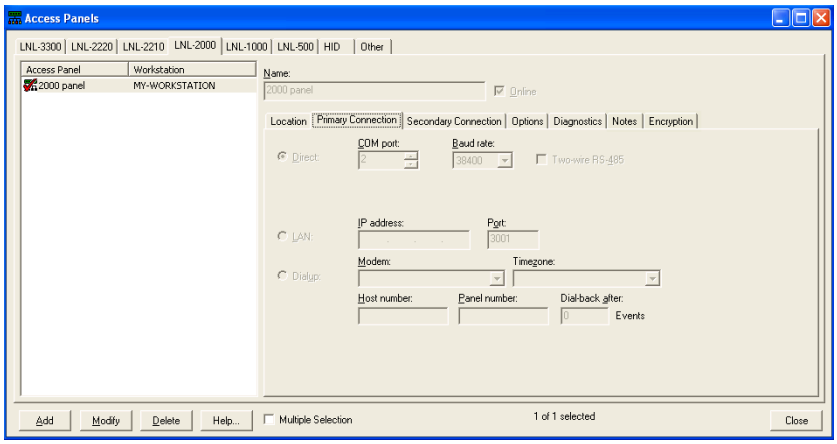
Mode
In view mode, indicates how many panels are currently selected, and the current total number of panels; for example, “2 of 5 selected”. In modify mode, indicates the current operation (Add Mode, Modify Mode, etc.).

Close
Closes the Access Panels folder.

LNL-2000 Form (Primary Connection Sub-tab)

Certain options on the Primary Connection and Secondary Connection tabs function together to limit combinations of primary and secondary communications for dual path usage. Valid dual path selections include:

Primary Connection option selected	Secondary Connection options available for selection
Direct	None, Direct, LAN, Dialup
LAN	None, Direct, LAN, Dialup
Dialup	None, Dialup



Direct

Select this radio button if communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**, the **Baud rate**, and whether or not communication to the host will use a **Two-wire RS-485** connection.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 through 255.

Baud rate

If you selected the **Direct** radio button, this is the speed (in bits per second) at which information is transferred between the workstation and the access panel via the serial connection.

Note: Some third party devices do not allow the baud rate to be modified from the host application software. If such a device is in use, the baud rate setting in OnGuard has no bearing. Refer to the documentation for any third party devices being used.

Two-wire RS-485

Other panels can be configured to communicate with the host workstation using either a 4-wire or 2-wire RS-485 connection. Select this check box if 2-wire communication is to be used.

LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's IP address.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator.

An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Dialup

Select this radio button if the workstation will communicate with the access panel using a dialup connection. This option functions together with the LAN option on the Secondary Connection sub-tab to limit combinations of primary and secondary communications for dual path usage.

You must also specify the workstation's modem, timezone, host number, panel number and dial-back after__events.

Modem

If you selected the **Dialup** radio button, select the modem on the workstation that will be used for dialup communication with the access panel. Choices include all TAPI (Telephone Application Programming Interface) devices that are currently configured on the specified Workstation.

Before a modem can be listed in this drop-down list, the modem must be properly configured for the selected workstation. This is done on the Modems form in the Dialup Configuration folder, which is reached by selecting ***Modems*** from the ***Access Control*** menu. For more information, refer to Connect a Modem to a Lenel Access Panel on page 704.

If any of the TAPI devices are used for other dial functions such as remote access, do not select them for panel dial usage. For more information, refer to your Windows user guide.

Timezone

If you selected the **Dialup** radio button, indicate the timezone during which the access panel will initiate dialup communication with the workstation. You can select only one timezone for the particular workstation-modem-panel combination. Timezones are defined on the Timezones form of the Timezones folder.

Functionally, at the start of each interval that comprises the timezone, the panel will automatically dial the host number. If a connection cannot be established, it will redial until a connection can be made. Once connected, all transactions stored in the panel will be dumped to the Communication Server (on the workstation) to be logged in the database. In addition, all commands that need to be sent to the panel will be sent from the host at that time.

After all information is transferred, the Communication Server will automatically terminate the dialup connection with the panel. The exception to this occurs if you select the "Always" timezone. In that situation, the workstation will attempt to always stay connected to the panel via dial-up. Functionally, this is similar to communicating with the workstation via a direct (serial) or LAN connection.

Multiple workstations can use the same TAPI modem, or one workstation might have access to multiple TAPI modems. However, only one connection to a particular modem can be established at a particular time. For example, a particular workstation might use a particular modem to dial one panel at 12:00, a second panel at 1:00, a third panel at 2:00, etc.

Host number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the workstation. This is the number that the access panel will use to dial into the panel to send events and other transactions to the workstation.

Type the exact dialing sequence here. Although you can use parentheses and dashes, they are ignored by TAPI devices. For example, 2489720 and (212) 546-1234. For more information, refer to your Windows user guide.

Panel number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the access panel. This is the number that the workstation would need to dial to communicate with the access panel.

Typically, all communication between the access panel and the workstation is initiated from the panel. However, the workstation can dial the panel from within the Alarm Monitoring system. This is done by right-clicking on the panel's entry in the System Tree, then selecting the **Connect** command from the popup menu. Any ASCII string can be typed here (for example, a comma typically triggers a pause in the dialing sequence).

Dial-back after__Events

This field is displayed only if you have selected the **Dialup** radio button.

LNL-2000 panels can be programmed to dial the workstation after a certain number of events have been stored in the panel but have not yet been reported to the host (because the panel has been offline).

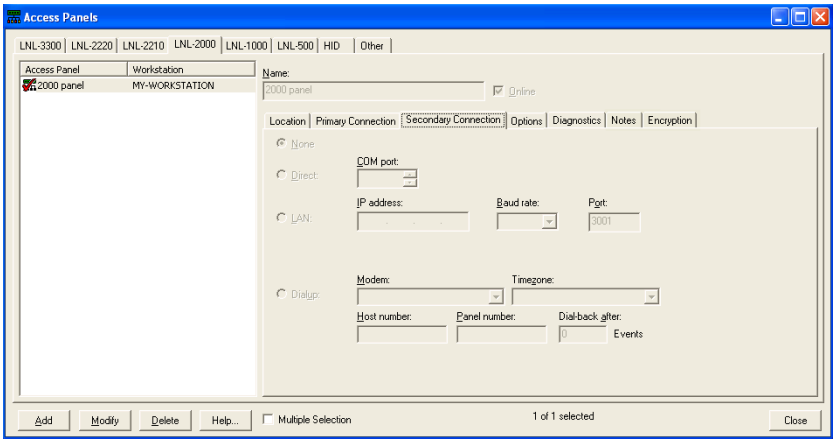
When the panel has accumulated the specified number of stored events, the panel will automatically dial the host number to dump its transactions and to receive any command programming. After the information has been exchanged, the workstation will terminate the connection.

The default value here is 255 events. The minimum value you can enter is zero (meaning that the panel will never dial the host). The maximum value is equal to one less than the maximum number of events that the panel can store.

LNL-2000 Form (Secondary Connection Sub-tab)

Certain options on the Secondary Connection and Primary Connection tabs function together to limit combinations of secondary and primary communications for dual path usage. Valid dual path selections include:

Secondary Connection option selected	Primary Connection options available for selection
Direct	Direct, LAN
LAN	Direct, LAN
Dialup	Direct, LAN, Dialup



None

Select if you want no secondary connection.

Direct

Select this radio button if for the secondary connection, communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 through 255.

LAN

Select this radio button if for the secondary connection the workstation will communicate with the access panel over a Local Area Network. This option functions together with the **Dialup** option on the Primary Connection sub-tab to limit combinations of primary and secondary communications for dual path usage. You must also specify the workstation's **IP address**.

IP address

If you selected the **LAN** radio button for secondary connection, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each

number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Baud rate

If you selected the **LAN** radio button, this field displays the speed (in bits per second) at which information is transferred between the workstation and the access panel via the serial connection. A baud rate of 38400 is automatically entered into this field when a **LAN** connection is selected. This value cannot be changed.

Note: Some third party devices do not allow the baud rate to be modified from the host application software. If such a device is in use, the baud rate setting in OnGuard has no bearing. Refer to the documentation for any third party devices being used.

Dialup

Select this radio button if for the secondary connection the workstation will communicate with the access panel using a dialup connection. You must also specify the workstation's **Modem**, **Timezone**, **Host number**, **Panel number** and **Dial-back after__Events**.

Modem

If you selected the **Dialup** radio button for secondary connection, select the modem on the workstation that will be used for dialup communication with the access panel. Choices include all TAPI (Telephone Application Programming Interface) devices that are currently configured on the specified **Workstation**.

Before a modem can be listed in this drop-down list, the modem must be properly configured for the selected **Workstation**. This is done on the Modems form in the Dialup Configuration folder, which is reached by selecting ***Modems*** from the ***Access Control*** menu. For more information, refer to Connect a Modem to a Lenel Access Panel on page 704. If any of the TAPI devices are used for other dial functions such as remote access, do not select them for panel dial usage. For more information, refer to your Windows user guide.

Timezone

If you selected the **Dialup** radio button for secondary connection, indicate the timezone during which the access panel will initiate dialup communication with the workstation.

You can select only one timezone for the particular workstation-modem-panel combination. Timezones are defined on the Timezones form of the Timezones folder.

Functionally, at the start of each interval that comprises the timezone, the LNL-2000 panel will automatically dial the **Host number**. If a connection cannot be established, it will redial until a connection can be made. Once connected, all transactions stored in the LNL-2000 will be dumped to the Communication Server (on the workstation) to be logged in the database. In addition, all commands that need to be sent to the LNL-2000 will be sent from the host at that time.

After all information is transferred, the Communication Server will automatically terminate the dialup connection with the LNL-2000 panel. The exception to this occurs if you select the "Always" timezone. In that situation, the workstation will attempt to always stay connected to the panel via dial-up. Functionally, this is similar to communicating with the workstation via a direct (serial) or LAN connection.

Multiple workstations can use the same TAPI modem, or one workstation might have access to multiple TAPI modems. However, only one connection to a particular modem can be established at a particular time. For example, a particular workstation might use a particular modem to dial one panel at 12:00, a second panel at 1:00, a third panel at 2:00, etc.

When the “Always” timezone is used as the dialup timezone for the secondary connection, the primary connection needs to be non-dialup (direct or LAN). When the primary connection is up, the secondary connection will be offline. If the primary connection goes down, a call will be placed to the panel on the secondary path after a certain period of time (default roughly 60 seconds). Once the secondary dialup connection has been established, the connection will remain until the primary connection has been re-established. After the primary connection is established, the secondary connection will remain connected for about one to two minutes (to make sure that the primary connection has connected and remained connected).

Host number

If you selected the **Dialup** radio button for secondary connection, enter the phone number used to reach the modem that’s connected to the workstation. This is the number that the access panel will use to dial into the panel to send events and other transactions to the workstation.

Type the exact dialing sequence here. Although you can use parentheses and dashes, they are ignored by TAPI devices. For example, 2489720 and (212) 546-1234. For more information, refer to your Windows user guide.

Panel number

If you selected the Dialup radio button for secondary connection, enter the phone number used to reach the modem that’s connected to the access panel. This is the number that the workstation would need to dial to communicate with the access panel.

Typically, all communication between the access panel and the workstation is initiated from the panel. However, the workstation can dial the panel from within the Alarm Monitoring system. This is done by right-clicking on the panel’s entry in the System Tree, then selecting the Connect command from the popup menu. Any ASCII string can be typed here (for example, a comma typically triggers a pause in the dialing sequence).

Dial-back after__Events

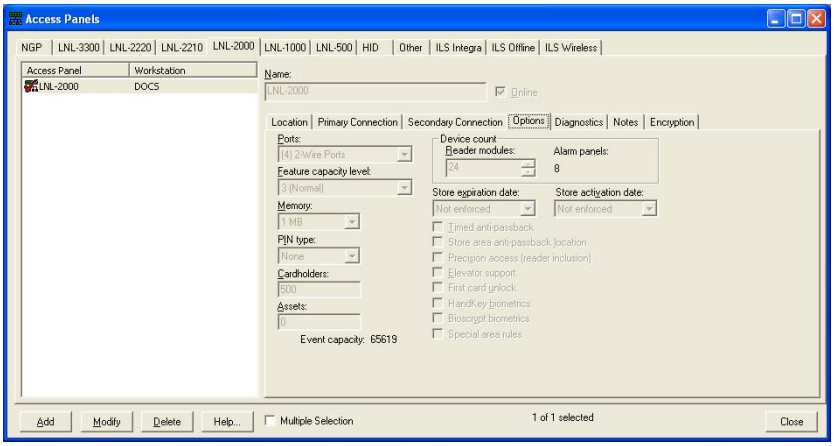
This field is displayed only if you have selected the Dialup radio button for secondary connection.

LNL-2000 panels can be programmed to dial the workstation after a certain number of events have been stored in the panel but have not yet been reported to the host (because the panel has been offline).

When the panel has accumulated the specified number of stored events, the panel will automatically dial the Host Number to dump its transactions and to receive any command programming. After the information has been exchanged, the workstation will terminate the connection.

The default value here is 255 events. The minimum value you can enter is zero (meaning that the panel will never dial the host). The maximum value is equal to one less than the maximum number of events that the panel can store.

LNL-2000 (Options Sub-tab)



Note: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

Ports

Access panels communicate with its downstream devices (reader interfaces, input control modules, and output control modules) using either 2- or 4-wire RS-485 communication, or a combination of the two.

Feature capacity level

This setting controls the amount of memory reserved for downstream devices, timezone control, local linkages, and other features within the controller. A higher value reserves more room for these options while leaving less room for the cardholder database and event transaction buffer.

In the vast majority of circumstances, the default value of 3 should be left unchanged. This value will rarely need to be adjusted. If free memory in the panel becomes low, flagged by a “Panel Free Memory Low” Alarm, this value should be increased.

Values of less than 3 are not recommended. They can be used in the rare case when there are few downstream devices, few configured features, and maximum memory is required for the cardholder database and/or event transaction buffer.

Memory

Indicates the amount of memory that’s on the panel.

To enable biometric support, you must have 76 bytes of available memory. Additional memory is required to store templates on the panel. For more information, refer to the Biometrics Form on page 402 (non-segmented systems) or the Segments Form (Biometrics Sub-tab) on page 466 (segmented systems).

Badge IDs require 4 to 8 bytes of memory, depending on the number of digits in a badge. For more information, refer to the Hardware Settings Form on page 398 (non-segmented systems) or the Segments Form (Hardware Settings Sub-tab) on page 463 (segmented systems).

PIN type

Select the range of PIN digits allowed. Using PINs takes up memory on the access panel, which reduces the card capacity.

If you have a pin code configured for a controller that is 1-n digits long, but have a cardholder in the database that has a pin code longer than n, the pin code gets downloaded with the badge record, but gets truncated at n digits. For example, you have a 1-4 digit pin for the controller, but the badge record in the access control system's database has '123456' specified as the pin code. When this gets downloaded, it is truncated to '1234.' The Cardholder can either enter the first 4 digits or all 6 digits correctly and gain access.

Cardholders

This field determines how much of the access panel's memory will be set aside for the cardholder records. This size is limited by the size of the access panel's memory, and is directly related to the options you choose in this section. The more options you choose and the more that each option requires (more digits in the card number, for example), the fewer the maximum number of cardholders possible.

Assets

Indicates the number of assets downloaded to the panels. To disable Asset Operations, set this value to 0.

Readers modules

Select the number of reader devices you plan to have attached to this LNL-2000 access panel. The more reader devices you have attached, the fewer alarm panels can be attached.

The actual number of readers that can be attached to the access panel is directly related to both the number of reader devices that are configured AND to the type of reader device(s) installed. Two readers can be attached to a Dual-Reader Interface board. One reader can be attached to a Single Reader Interface board.

You can choose a value in the range of 16 through 32. The value in the **Alarm panels** field is adjusted accordingly. The total number of devices (readers modules + alarm panels) cannot exceed 32.

Alarm panels

Indicates the maximum number of alarm panels that can be attached to this LNL-2000 access panel. You can change this field only indirectly, by modifying the **Readers modules** field on this form. The more readers you have attached, the fewer alarm panels can be attached.

Store expiration date

If you want the badge expiration date to be used to determine the status of cards detected at the card readers, select "Date only" from the drop-down list. If the present date is later than the expiration date of the card, the card is considered to be invalid and access is denied.

If you do not want the badge expiration date to be used to determine the status of card, select "Not enforced" from the drop-down list.

A third option, "Date and time" is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge expiration date and time to be used to determine the status of cards detected at readers. If the present date and time is later than the expiration date and time of the card, the card is considered to be invalid and access is denied.

Store activation date

If you want the badge activation date to be used to determine the status of cards detected at the card readers, select "Date only" from the drop-down list. If the present date is earlier than the activation date of the card, the card is considered invalid and access is denied.

If you do not want the badge activation date to be used to determine the status of card, select "Not enforced" from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge activation date and time to be used to determine the status of cards detected at readers. If the present date and time is earlier than the activation date and time of the card, the card is considered to be invalid and access is denied.

Timed anti-passback

Indicates that readers attached to this panel are to be used for timed anti-passback. You must also set the **Timed anti-passback setting (minutes)** field. This is done on the Anti-Passback form of the Readers folder.

Store area anti-passback location

Select this check box if a reader attached to this access panel is used to enter or leave an anti-passback area. Anti-passback areas are defined on the Anti-Passback Areas form of the Areas folder. The **Area entering** and **Area leaving** fields, located on the Anti-Passback form of the Readers folder, are used to associate specific readers with specific areas.

Precision access (reader inclusion)

If selected, it indicates that this access panel will use the application’s precision access capabilities. Precision access is a method for assigning unique access privileges to individual cardholders. There is an infinite number of precision access combinations that can be created and assigned to cardholders.

Note: Using this option severely limits the number of cardholders that can be stored in the panel. If you wish to use precision access, it is recommended that panel memory be expanded to meet your facility’s needs.

Elevator support

If selected, this panel will support elevator control. You must have at least 1 MB of memory to use this feature. This check box will be grayed out if 256 KB of memory is used.

First card unlock

If selected, this panel will have first card unlock functionality. First card unlock is used in conjunction with reader mode and timezone control. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.

Note: If the reader is in “Facility code only” mode, the first card unlock feature does not work.

HandKey biometrics

Enables hand geometry (HandKey) support. Specifically, this check box enables alternate readers to download templates to the panel.

76 bytes of memory are required to enable hand geometry support, and additional memory is required to store template information on the panel. For more information, refer to the System Options folder (non-segmented systems) or the Segments folder (segmented systems).

Note: The **Maximum templates** setting must be greater than zero (the default value) for the panel to support HandKey alternate readers. This setting is located on the System Options folder > Biometrics form (non-segmented systems) or the Segments form > Biometrics sub-tab (segmented systems).

Bioscrypt biometrics

Enables Bioscrypt alternate reader support. Specifically, this check box enables alternate readers to download templates to the panel.

76 bytes of memory are required to enable Bioscrypt biometric support, and additional memory is required to store template information on the access panel. For more information, refer to the System Options folder (non-segmented systems) or the Segments folder (segmented systems).

Note: The **Maximum templates** setting must be greater than zero (the default value) for the panel to support Bioscrypt alternate readers. This setting is located on the System Options folder > Biometrics form (non-segmented systems) or the Segments form > Biometrics sub-tab (segmented systems).

Special area rules

Checking this option enables the Special Two-Man Rule. If this is the first time enabling this rule a check will be made on your system and a message displayed informing you that additional changes may have to be made to the cardholder badge options. For more information please refer to Appendix G: Special Two-Man Rule on page 1435.

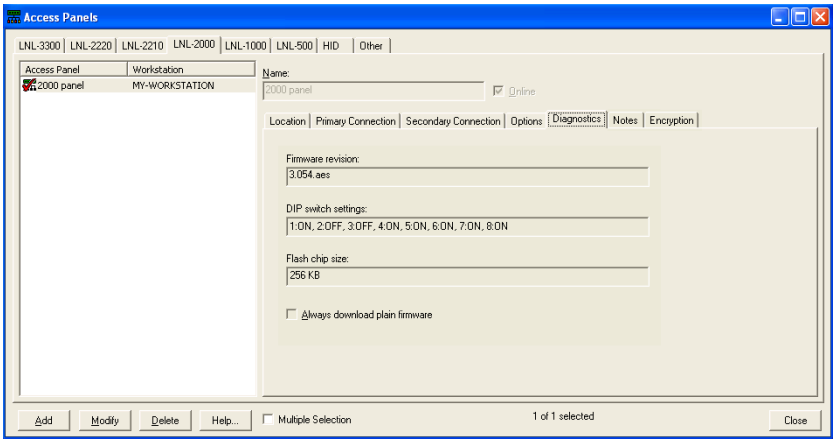
Event capacity

Calculates and displays the number of events that can be stored on the panel based on the parameters you've selected. The minimum is 1000 events. The memory usage in an access panel is based on two criteria:

- Memory used for cardholder storage
- Memory used for event history storage

After cardholder storage requirements are computed based on the options selected in this section, all remaining memory is used for event storage.

LNL-2000 (Diagnostics Sub-tab)



Firmware revision

Displays the firmware revision reported by the controller the last time it was online. This is a read only text field.

DIP switch settings

Displays the DIP switch settings reported by the controller, the last time it was online. This is a read only text field. Note that DIP switch settings are read by the controller only when the controller is powered up. DIP switch changes made afterward will not take affect until the controller goes through another power cycle.

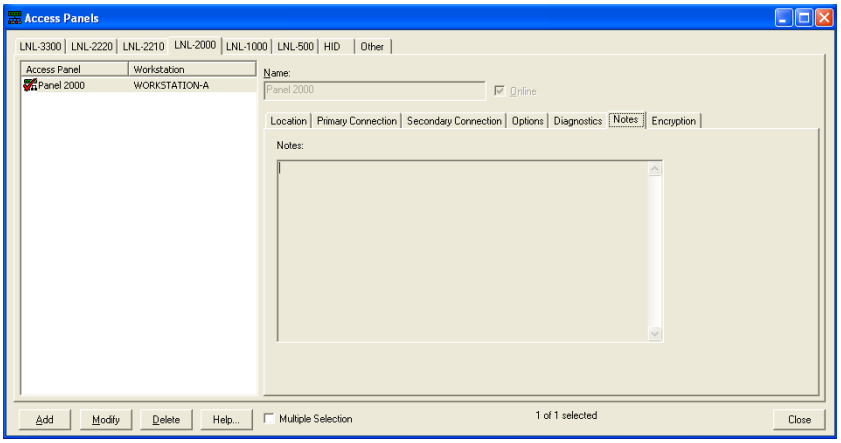
Flash chip size

Displays the flash chip size (always 256 KB for the LNL-2000) reported by the controller, the last time it was online. This is a read only text field.

Always download plain firmware

Determines the type of firmware downloaded to the controller. If not selected, (the default) the system downloads AES/Extended firmware to the controller. If selected, the system downloads plain firmware to the controller.

LNL-2000 (Notes Sub-tab)



Notes

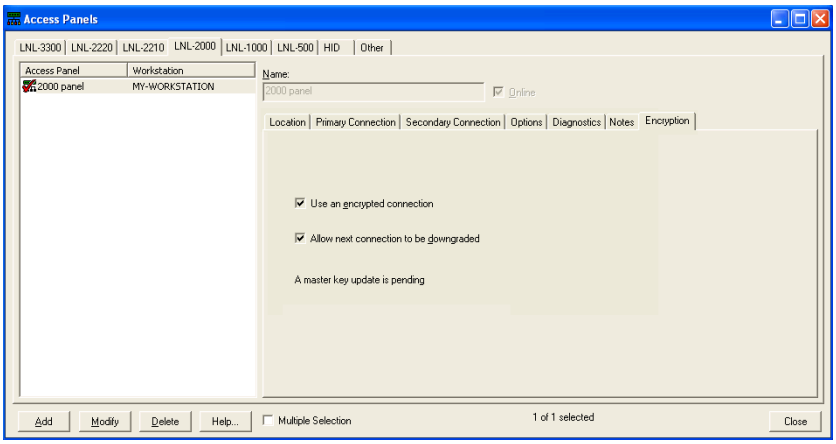
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

LNL-2000 (Encryption Sub-tab)

This view displays when the system/segment (the panel is associated with) uses automatic encryption. The same fields display when the system/segment is configured for manual encryption, except for the **Allow next connection to be downgraded** check box.The Encryption sub-tab does not display if a system/segment uses a plain connection.

Note: The system/segment the controller belongs to must be configured for encryption in order for this tab to display. The user must also have the correct user permissions.

For more information about encryption, refer to the Encryption for Controllers User Guide.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key, the factory default master keys, and finally by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible.

This check box displays only if the controller exists in an automatic key management system/segment.

A custom key update is pending

Indicates there is an outstanding key update for this controller. This is a read only field. This text field displays only if the controller exists in an automatic key management system/segment, and the condition exists (if there is an outstanding key update).

LNL-2000 Form Procedures

Add an LNL-2000 Access Panel

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu. Click the LNL-2000 tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the access panel.
4. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system or defining panels, but instead would wait until you're ready to put the panel into service.
5. Specify communication parameters on the Location, Primary Connection, and Secondary Connection sub-tabs.

6. Specify setup parameters on the Options sub-tab, which sets up the cardholder database for this panel.

   IMPORTANT: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

7. Click [OK].

Modify an LNL-2000 Access Panel

Notes: Modifying the PIN type requires a full panel download.

If the PIN type is modified on the controller and/or the General Cardholder Options form, you must log off/log on to System Administration before you modify a cardholder pin number.

1. In the listing window, select the LNL-2000 entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an LNL-2000 Access Panel

1. In the listing window, select the LNL-2000 entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enable an LNL-2000 Access Panel for Encryption

The encryption modify/export permission is required to complete this procedure.

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu.
2. On the LNL-2000 form, click the Encryption sub-tab.
3. In the listing window, select the LNL-2000 entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

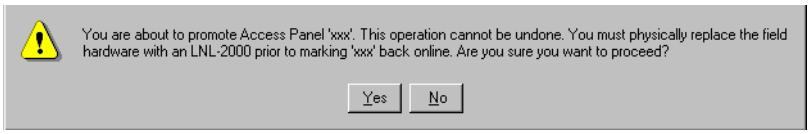
Promote an LNL-2000 Access Panel to an LNL-2210, LNL-2220, or LNL-3300

Note: In order to promote an access panel, it must be offline.

In order to promote an access panel to an LNL-2210 the panel's Primary Connection must be configured as a LAN type. In addition, you may need to configure the panel's existing devices to conform with one of the configurations supported by the LNL-2210:

- Up to 8 downstream RS-485 devices (readers modules and alarm panels)
- Up to 17 readers (using 8 dual reader interface modules and 1 onboard reader).

1. In the listing window, right-click over the LNL-2000 entry you wish to promote.
2. From the pop-up menu, select **Promote Access Panel to LNL-2210**, **Promote Access Panel to LNL-2200**, or **Promote Access Panel to LNL-3300**. The following message will be displayed:



3. Click [Yes] to continue.
4. Click [OK].

Enter Notes for an Access Panel

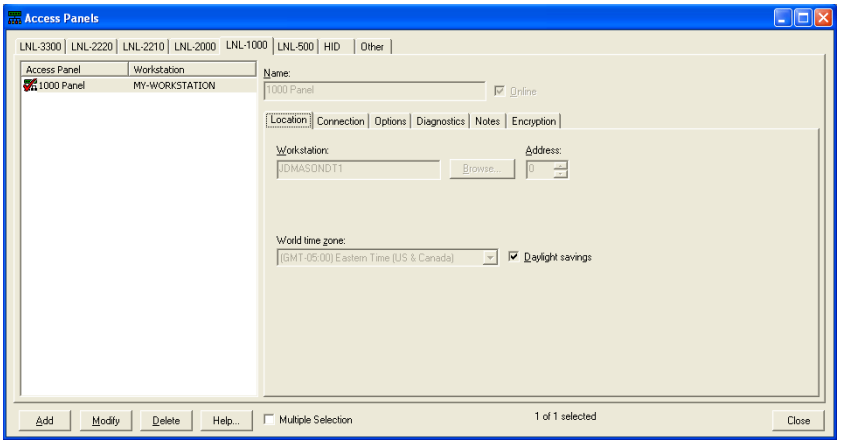
1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

LNL-1000 Form Overview

This form is used to:

- Assign names to individual LNL-1000 type access panels in the software
- Specify access panel setup parameters, including information stored in the panel
- Specify communication panel setup parameters, including the workstation associated with the panel and the access method (direct serial connection, LAN, or dialup)
- View the firmware, DIP switch settings and flash chip size of the panel
- Enable encryption, if you have the proper user permission

LNL-1000 Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the access panel. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Selects the workstation or server to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation.You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Note: You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

Address

Specifies the panel’s address, which must match the DIP switch setting on the panel itself. Possible values are in the range of 0 through 7. The factory default DIP switch setting is 0.

Note: For any panel(s) that will be communicating with a workstation using a dialup connection, the panel(s) must be set to address 1 or the dial-back to host capability will fail.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Add

Adds a panel entry.

Modify

Changes a panel entry.

Delete

Removes a panel entry.

Help

Displays online help for this topic.

Change Segment

Displays if segmentation is enabled and you are in modify mode. Click this button to move the access panel to a different segment.

Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected panels.

Mode

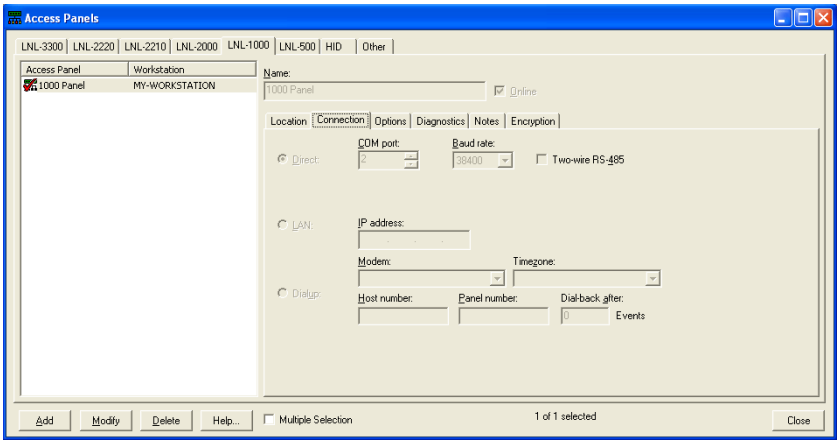
In view mode, indicates how many panels are currently selected, and the current total number of panels; for example, "2 of 5 selected".

In modify mode, indicates the current operation (Add Mode, Modify Mode, etc.).

Close

Closes the Access Panels folder.

LNL-1000 Form (Connection Sub-tab)



Direct

Select this radio button if communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**, the **Baud rate**, and whether or not communication to the host will use a **Two-wire RS-485** connection.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 through 255.

Baud rate

If you selected the **Direct** radio button, this is the speed (in bits per second) at which information is transferred between the workstation and the access panel via the serial connection.

Note: Some third party devices do not allow the baud rate to be modified from the host application software. If such a device is in use, the baud rate setting in OnGuard has no bearing. Refer to the documentation for any third party devices being used.

Two-wire RS-485

The panel can be configured to communicate with the host workstation using either a 4-wire or 2-wire RS-485 connection. Select this check box if 2-wire communication is to be used.

LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's **IP address**.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Dialup

Select this radio button if the workstation will communicate with the access panel using a dialup connection. This option functions together with the **LAN** option on the Secondary Connection sub-tab to limit combinations of primary and secondary communications for dual path usage.

You must also specify the workstation's **Modem**, **Timezone**, **Host number**, **Panel number** and **Dial-back after__Events**.

Modem

If you selected the **Dialup** radio button, select the modem on the workstation that will be used for dialup communication with the access panel. Choices include all TAPI (Telephone Application Programming Interface) devices that are currently configured on the specified **Workstation**.

Before a modem can be listed in this drop-down list, the modem must be properly configured for the selected **Workstation**. This is done on the Modems form in the Dialup Configuration folder, which is reached by selecting ***Modems*** from the ***Access Control*** menu. For more information, refer to Connect a Modem to a Lenel Access Panel on page 704. If any of the TAPI devices are used for other dial functions such as remote access, do not select them for panel dial usage. For more information, refer to your Windows user guide.

Timezone

If you selected the **Dialup** radio button, indicate the timezone during which the access panel will initiate dialup communication with the workstation. You can select only one timezone for the particular workstation-modem-panel combination. Timezones are defined on the Timezones form of the Timezones folder.

Functionally, at the start of each interval that comprises the timezone, the panel will automatically dial the **Host Number**. If a connection cannot be established, it will redial until a connection can be made. Once connected, all transactions stored in the panel will be dumped to the Communication Server (on the workstation) to be logged in the database. In addition, all commands that need to be sent to the panel will be sent from the host at that time.

After all information is transferred, the Communication Server will automatically terminate the dialup connection with the panel. The exception to this occurs if you select the "Always" timezone. In that situation, the workstation will attempt to always stay connected to the panel via dial-up. Functionally, this is similar to communicating with the workstation via a direct (serial) or LAN connection.

Multiple workstations can use the same TAPI modem, or one workstation might have access to multiple TAPI modems. However, only one connection to a particular modem can be established at a particular time. For example, a particular workstation might use a particular modem to dial one panel at 12:00, a second panel at 1:00, a third panel at 2:00, etc.

Host number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the workstation. This is the number that the access panel will use to dial into the panel to send events and other transactions to the workstation.

Type the exact dialing sequence here. Although you can use parentheses and dashes, they are ignored by TAPI devices. For example, 2489720 and (212) 546-1234. For more information, refer to your Windows user guide.

Panel number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the access panel. This is the number that the workstation would need to dial to communicate with the access panel.

Typically, all communication between the access panel and the workstation is initiated from the panel.

However, the workstation can dial the panel from within the Alarm Monitoring system. This is done by right-clicking on the panel's entry in the System Tree, then selecting the **Connect** command from the popup menu.

Any ASCII string can be typed here (for example, a comma typically triggers a pause in the dialing sequence).

Dial-back after__Events

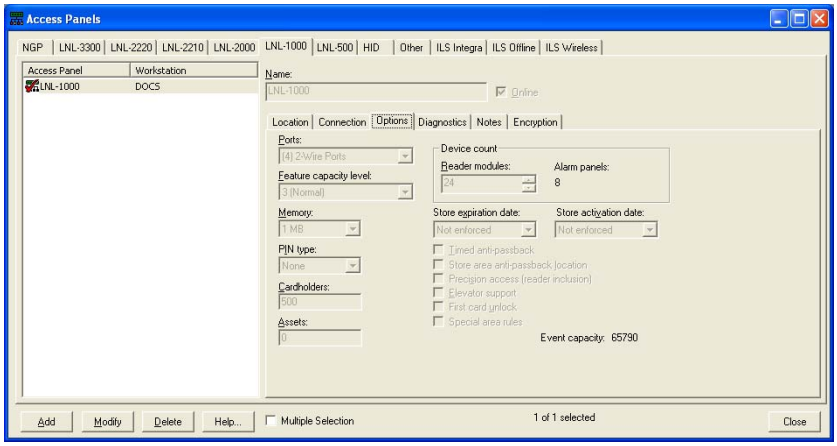
This field is displayed only if you have selected the **Dialup** radio button.

Panels can be programmed to dial the workstation after a certain number of events have been stored in the panel but have not yet been reported to the host (because the panel has been offline).

When the panel has accumulated the specified number of stored events, the panel will automatically dial the **Host Number** to dump its transactions and to receive any command programming. After the information has been exchanged, the workstation will terminate the connection.

The default value here is 255 events. The minimum value you can enter is zero (meaning that the panel will never dial the host). The maximum value is equal to one less than the maximum number of events that the panel can store.

LNL-1000 Form (Options Sub-tab)



Note: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

Ports

Access panels communicate with downstream devices (reader interfaces, input control modules, and output control modules) using either 2- or 4-wire RS-485 communication, or a combination of the two.

Feature capacity level

This setting controls the amount of memory reserved for downstream devices, timezone control, local linkages, and other features within the controller. A higher value reserves more room for these options while leaving less room for the cardholder database and event transaction buffer.

In the vast majority of circumstances, the default value of 3 should be left unchanged. This value will rarely need to be adjusted. If free memory in the panel becomes low, flagged by a “Panel Free Memory Low” Alarm, this value should be increased.

Values of less than 3 are not recommended. They can be used in the rare case when there are few downstream devices, few configured features, and maximum memory is required for the cardholder database and/or event transaction buffer.

Memory

Indicates the amount of memory that’s on the panel. To use the Elevator Control features, you must have 1 MB or more of memory.

PIN type

Select the range of PIN digits allowed. Using PINs takes up memory on the access panel, which reduces the card capacity.

If you have a pin code configured for a controller that is 1-n digits long, but have a cardholder in the database that has a pin code longer than n, the pin code gets downloaded with the badge record, but gets truncated at n digits. For example, you have a 1-4 digit pin for the controller, but the badge record in the access control system’s database has ‘123456’ specified as the pin code. When this gets downloaded, it is truncated to ‘1234.’ The Cardholder can either enter the first 4 digits or all 6 digits correctly and gain access.

Cardholders

This field determines how much of the access panel’s memory will be set aside for the cardholder records. This size is limited by the size of the access panel’s memory, and is directly related to the options you choose in this section. The more options you choose and the more that each option requires (more digits in the card number, for example), the fewer the maximum number of cardholders possible.

Assets

Indicates the number of assets downloaded to panels. To disable Asset Operations, set this value to 0. You must have at least 1 MB of memory to use this feature. This field will be grayed out if 256 KB of memory is used.

Readers modules

Select the number of reader devices you plan to have attached to this access panel. The more reader devices you have attached, the fewer alarm panels can be attached.

The actual number of readers that can be attached to the access panel is directly related to both the number of reader devices that are configured AND to the type of reader device(s) installed. Two readers can be attached to a Dual-Reader Interface board. One reader can be attached to a Single Reader Interface board.

You can choose a value in the range of 16 through 32. The value in the **Alarm panels** field is adjusted accordingly. The total number of devices (reader modules + alarm panels) cannot exceed 32.

Alarm panels

Indicates the maximum number of alarm panels that can be attached to this access panel. You can change this field only indirectly, by modifying the **Readers modules** field on this form. The more readers you have attached, the fewer alarm panels can be attached.

Store expiration date

If you want the badge expiration date to be used to determine the status of cards detected at the card readers, select “Date only” from the drop-down list. If the present date is later than the expiration date of the card, the card is considered to be invalid and access is denied.

If you do not want the badge expiration date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge expiration date and time to be used to determine the status of cards detected at readers. If the present date and time is later than the expiration date and time of the card, the card is considered to be invalid and access is denied.

Store activation date

If you want the badge activation date to be used to determine the status of cards detected at the card readers, select “Date only” from the drop-down list. If the present date is earlier than the activation date of the card, the card is considered invalid and access is denied.

If you do not want the badge activation date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge activation date and time to be used to determine the status of cards detected at readers. If the present date and time is earlier than the activation date and time of the card, the card is considered to be invalid and access is denied.

Timed anti-passback

Indicates that readers attached to this panel are to be used for timed anti-passback. You must also set the **Timed anti-passback setting (minutes)** field. This is done on the Anti-Passback form of the Readers folder.

Store area anti-passback location

Select this check box if a reader attached to this access panel is used to enter or leave an anti-passback area. Anti-passback areas are defined on the Anti-Passback Areas form of the Areas folder. The **Area entering** and **Area leaving** fields, located on the Anti-Passback form of the Readers folder, are used to associate specific readers with specific areas.

Precision access (reader inclusion)

If selected, it indicates that this access panel will use the application’s precision access capabilities. Precision access is a method for assigning unique access privileges to individual cardholders. There is an infinite number of precision access combinations that can be created and assigned to cardholders.

Note: Using this option severely limits the number of cardholders that can be stored in the panel. If you wish to use precision access, it is recommended that panel memory be expanded to meet your facility’s needs.

Elevator support

If selected, this panel will support elevator control. You must have at least 1 MB of memory to use this feature. This check box will be grayed out if 256 KB of memory is used.

First card unlock

If selected, this panel will have first card unlock functionality.

First card unlock is used in conjunction with reader mode and timezone control. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.

Note: If the reader is in “Facility code only” mode, the first card unlock feature does not work.

Special area rules

When checked this option enables the Special Two-Man Rule. If this is the first time enabling this rule a check will be made on your system and a message displayed informing you that additional changes may have to be made to the cardholder badge options. For more information please refer to Appendix G: Special Two-Man Rule on page 1435.

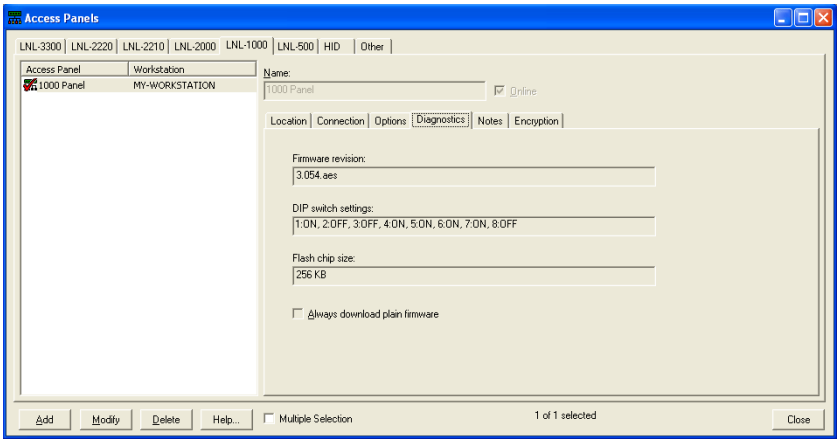
Event capacity

Calculates and displays the number of events that can be stored on the panel based on the parameters you’ve selected. The minimum is 1000 events. The memory usage in an access panel is based on two criteria:

- Memory used for cardholder storage
- Memory used for event history storage

After cardholder storage requirements are computed based on the options selected in this section, all remaining memory is used for event storage.

LNL-1000 Form (Diagnostics Sub-tab)



Firmware revision

Displays the firmware revision reported by the controller the last time it was online. This is a read only text field.

DIP switch settings

Displays the DIP switch settings reported by the controller, the last time it was online. This is a read only text field. Note that DIP switch settings are read by the controller only when the controller is powered up. DIP switch changes made afterward will not take affect until the controller goes through another power cycle.

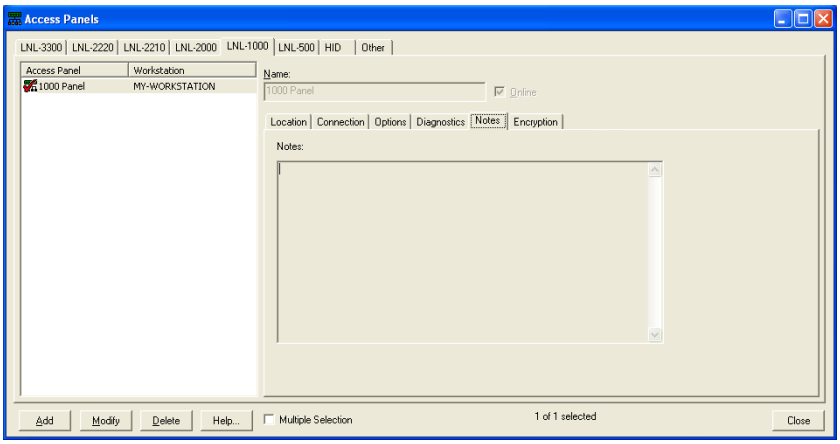
Flash chip size

Displays the flash chip size (128 KB or 256 KB) reported by the controller, the last time it was online. This is a read only text field.

Always download plain firmware

Determines the type of firmware downloaded to the controller. If not selected, (the default) the system downloads AES/Extended firmware to the controller whenever the controller has a 256 KB flash chip. If selected, the system always downloads plain firmware to the controller.

LNL-1000 Form (Notes Sub-tab)



Notes

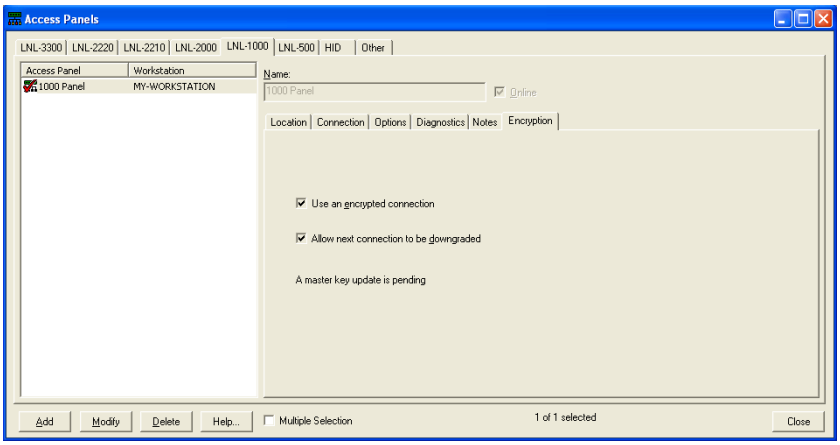
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

LNL-1000 Form (Encryption Sub-tab)

This view displays when the system/segment (the panel is associated with) uses automatic encryption. When the system/segment is configured for manual encryption, the same fields display except for the **Allow next connection to be downgraded** check box.The Encryption sub-tab does not display if a system/segment uses a plain connection.

Note: The system/segment the controller belongs to must be configured for encryption in order for this tab to display. The user must also have the correct user permissions.

For more information about encryption, refer to the Encryption for Controllers User Guide.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key, the factory default master keys, and finally by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible. This check box displays only if the controller exists in an automatic key management system/segment.

A custom key update is pending

Indicates there is an outstanding key update for this controller. This is a read only field. This text field displays only if the controller exists in an automatic key management system/segment, and the condition exists (if there is an outstanding key update).

LNL-1000 Form Procedures

Add an LNL-1000 Access Panel

IMPORTANT: If you want to configure (add) several access panels, use the Configure Access Panels Wizard which is available by selecting ***Wizards*** from the ***Application*** menu. The wizard provides detailed instructions to guide you through the configuration process. The wizard is only available for LNL-1000 access panels.

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu. Click the LNL-1000 tab.
2. Click [Add].
3. In the **Name** field, enter a unique, descriptive name for the access panel.

4. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system or defining panels, but instead would wait until you're ready to put the panel into service.
5. Specify communication parameters on the Location and Connection sub-tabs.
6. Specify setup parameters on the Options sub-tab, which sets up the cardholder database for this panel.

   IMPORTANT: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

7. Click [OK].

Modify an LNL-1000 Access Panel

Notes: Modifying the PIN type requires a full panel download.

If the PIN type is modified on the controller and/or the General Cardholder Options form, you must log off/log on to System Administration before you modify a cardholder pin number.

1. In the listing window, select the LNL-1000 entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an LNL-1000 Access Panel

1. In the listing window, select the LNL-1000 entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enable an LNL-1000 Access Panel for Encryption

The encryption modify/export permission is required to complete this procedure.

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu. Click the LNL-1000 tab.
2. Click the Encryption sub-tab.
3. In the listing window, select the LNL-1000 entry you wish to change.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the next connection to downgrade to a plain connection if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Promote an LNL-1000 Access Panel to an LNL-2000, LNL-2210, LNL-2220, or LNL-3300

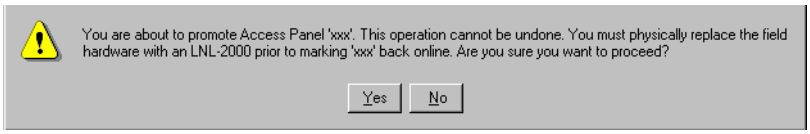
Note: In order to promote an access panel, it must be offline.

In order to promote an access panel to an LNL-2210 the panel's Primary Connection must be configured as a LAN type. In addition, you may need to configure the panel so that it conforms to one of the configurations supported by the LNL-2210:

- Up to 8 downstream RS-485 devices (readers modules and alarm panels)
- Up to 17 readers (using 8 dual reader interface modules and 1 onboard reader).

1. In the listing window, right-click over the LNL-1000 entry you wish to promote.

From the pop-up menu, select **Promote Access Panel to LNL-2000**, **Promote Access Panel to LNL-2210**, **Promote Access Panel to LNL-2220**, or **Promote Access Panel to LNL-3300**. The following message will be displayed:



2. Click [Yes] to continue.
3. Click [OK].

Enter Notes for an Access Panel

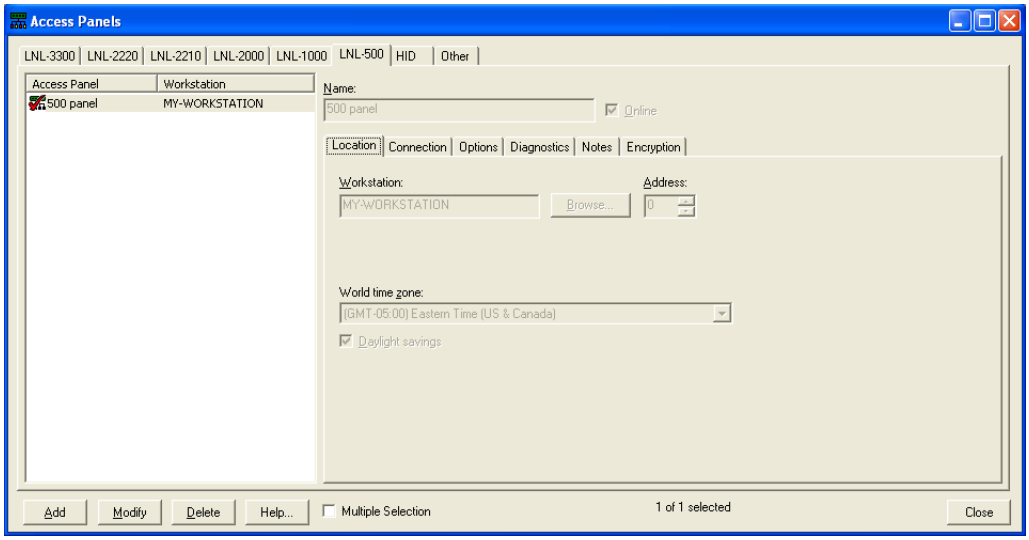
1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

LNL-500 Form Overview

This form is used to:

- Assign names to individual LNL-500 type access panels in the software
- Specify access panel setup parameters, including information stored in the panel
- Specify communication panel setup parameters, including the workstation associated with the panel and the access method (direct serial connection, LAN, or dialup)
- View the firmware, DIP switch settings and flash chip size of the panel
- Enable encryption, if you have the proper user permission

LNL-500 Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the access panel. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Selects the workstation or server to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Note: You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

Address

Specifies the panel’s address, which must match the DIP switch setting on the panel itself. Possible values are in the range of 0 through 7. The factory default DIP switch setting is 0.

Note: For any panel(s) that will be communicating with a workstation using a dialup connection, the panel(s) must be set to address 1 or the dial-back to host capability will fail.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Add

Adds a panel entry.

Modify

Changes a panel entry.

Delete

Removes a panel entry.

Help

Displays online help for this topic.

Change Segment

Displays if segmentation is enabled and you are in modify mode. Click this button to move the access panel to a different segment.

Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected panels.

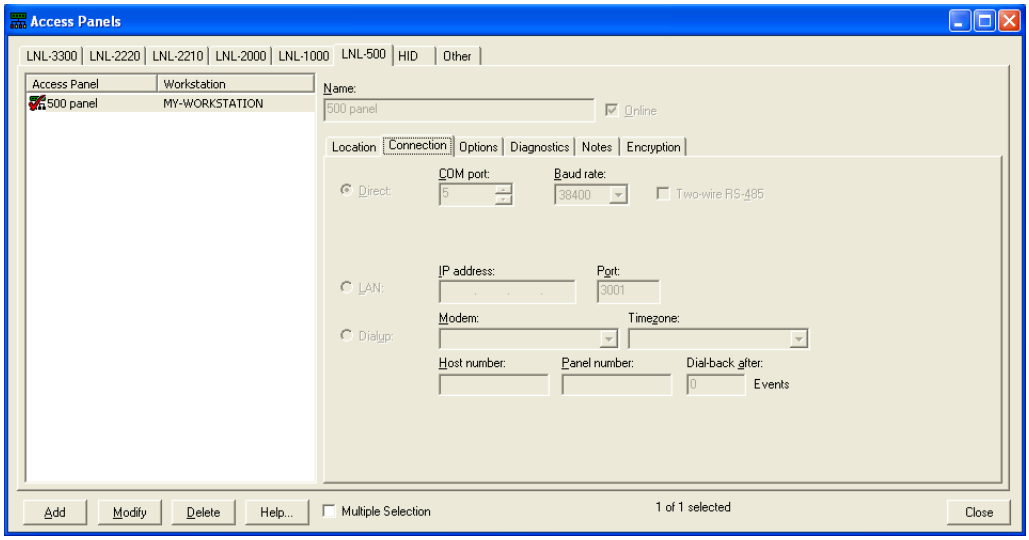
Mode

In view mode, indicates how many panels are currently selected, and the current total number of panels; for example, "2 of 5 selected". In modify mode, indicates the current operation (Add Mode, Modify Mode, etc.).

Close

Closes the Access Panels folder.

LNL-500 Form (Connection Sub-tab)



Direct

Select this radio button if communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**, the **Baud rate**, and whether or not communication to the host will use a **Two-wire RS-485** connection.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 through 255.

Baud rate

If you selected the **Direct** radio button, this is the speed (in bits per second) at which information is transferred between the workstation and the access panel via the serial connection.

Note: Some third party devices do not allow the baud rate to be modified from the host application software. If such a device is in use, the baud rate setting in OnGuard has no bearing. Refer to the documentation for any third party devices being used.

Two-wire RS-485

The panel can be configured to communicate with the host workstation using either a 4-wire or 2-wire RS-485 connection. Select this check box if 2-wire communication is to be used.

LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's **IP address**.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Dialup

Select this radio button if the workstation will communicate with the access panel using a dialup connection. This option functions together with the **LAN** option on the Secondary Connection sub-tab to limit combinations of primary and secondary communications for dual path usage. You must also specify the workstation's **Modem**, **Timezone**, **Host number**, **Panel number** and **Dial-back after__Events**.

Modem

If you selected the **Dialup** radio button, select the modem on the workstation that will be used for dialup communication with the access panel. Choices include all TAPI (Telephone Application Programming Interface) devices that are currently configured on the specified **Workstation**.

Before a modem can be listed in this drop-down list, the modem must be properly configured for the selected **Workstation**. This is done on the Modems form in the Dialup Configuration folder, which is reached by selecting ***Modems*** from the ***Access Control*** menu. For more information, refer to Connect a Modem to a Lenel Access Panel on page 704. If any of the TAPI devices are used for other dial functions such as remote access, do not select them for panel dial usage. For more information, refer to your Windows user guide.

Timezone

If you selected the **Dialup** radio button, indicate the timezone during which the access panel will initiate dialup communication with the workstation. You can select only one timezone for the particular workstation-modem-panel combination. Timezones are defined on the Timezones form of the Timezones folder.

Functionally, at the start of each interval that comprises the timezone, the panel will automatically dial the **Host Number**. If a connection cannot be established, it will redial until a connection can be made. Once connected, all transactions stored in the panel will be dumped to the Communication Server (on the workstation) to be logged in the database. In addition, all commands that need to be sent to the panel will be sent from the host at that time.

After all information is transferred, the Communication Server will automatically terminate the dialup connection with the panel. The exception to this occurs if you select the "Always" timezone. In that situation, the workstation will attempt to always stay connected to the panel via dial-up. Functionally, this is similar to communicating with the workstation via a direct (serial) or LAN connection.

Multiple workstations can use the same TAPI modem, or one workstation might have access to multiple TAPI modems. However, only one connection to a particular modem can be established at a particular time. For example, a particular workstation might use a particular modem to dial one panel at 12:00, a second panel at 1:00, a third panel at 2:00, etc.

Host number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the workstation. This is the number that the access panel will use to dial into the panel to send events and other transactions to the workstation.

Type the exact dialing sequence here. Although you can use parentheses and dashes, they are ignored by TAPI devices. For example, 2489720 and (212) 546-1234. For more information, refer to your Windows user guide.

Panel number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the access panel. This is the number that the workstation would need to dial to communicate with the access panel.

Typically, all communication between the access panel and the workstation is initiated from the panel.

However, the workstation can dial the panel from within the Alarm Monitoring system. This is done by right-clicking on the panel's entry in the System Tree, then selecting the **Connect** command from the popup menu.

Any ASCII string can be typed here (for example, a comma typically triggers a pause in the dialing sequence).

Dial-back after__Events

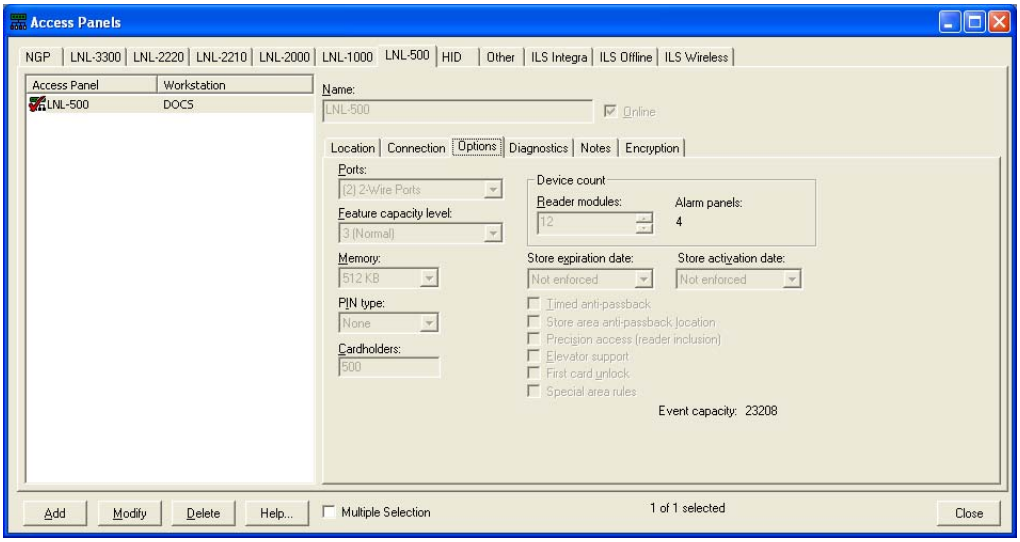
This field is displayed only if you have selected the **Dialup** radio button.

Panels can be programmed to dial the workstation after a certain number of events have been stored in the panel but have not yet been reported to the host (because the panel has been offline).

When the panel has accumulated the specified number of stored events, the panel will automatically dial the **Host Number** to dump its transactions and to receive any command programming. After the information has been exchanged, the workstation will terminate the connection.

The default value here is 255 events. The minimum value you can enter is zero (meaning that the panel will never dial the host). The maximum value is equal to one less than the maximum number of events that the panel can store.

LNL-500 Form (Options Sub-tab)



Note: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

Ports

Access panels communicate with downstream devices (reader interfaces, input control modules, and output control modules) using either 2- or 4-wire RS-485 communication.

Feature capacity level

This setting controls the amount of memory reserved for downstream devices, timezone control, local linkages, and other features within the controller. A higher value reserves more room for these options while leaving less room for the cardholder database and event transaction buffer.

In the vast majority of circumstances, the default value of 3 should be left unchanged. This value will rarely need to be adjusted. If free memory in the panel becomes low, flagged by a “Panel Free Memory Low” Alarm, this value should be increased.

Values of less than 3 are not recommended. They can be used in the rare case when there are few downstream devices, few configured features, and maximum memory is required for the cardholder database and/or event transaction buffer.

Memory

Indicates the amount of memory that’s on the panel. The LNL-500 has 512 KB of memory and this value cannot be changed.

PIN type

Select the range of PIN digits allowed. Using PINs takes up memory on the access panel, which reduces the card capacity.

If you have a pin code configured for a controller that is 1-n digits long, but have a cardholder in the database that has a pin code longer than n, the pin code gets downloaded with the badge record, but gets truncated at n digits. For example, you have a 1-4 digit pin for the controller, but the badge record in the access control system’s database has ‘123456’ specified as the pin code. When this gets downloaded, it is truncated to ‘1234.’ The Cardholder can either enter the first 4 digits or all 6 digits correctly and gain access.

Cardholders

This field determines how much of the access panel’s memory will be set aside for the cardholder records. This size is limited by the size of the access panel’s memory, and is directly related to the options you choose in this section. The more options you choose and the more that each option requires (more digits in the card number, for example), the fewer the maximum number of cardholders possible.

Assets

Indicates the number of assets downloaded to the panels. To disable Asset Operations, set this value to 0.

Readers modules

Select the number of reader devices you plan to have attached to this access panel. The more reader devices you have attached, the fewer alarm panels can be attached.

The actual number of readers that can be attached to the access panel is directly related to both the number of reader devices that are configured AND to the type of reader device(s) installed. Two readers can be attached to a Dual-Reader Interface board. One reader can be attached to a Single Reader Interface board.

You can choose a value in the range of 8 through 16. The value in the **Alarm panels** field is adjusted accordingly. The total number of devices (reader modules + alarm panels) cannot exceed 16.

Alarm panels

Indicates the maximum number of alarm panels that can be attached to this access panel. You can change this field only indirectly, by modifying the **Readers modules** field on this form. The more readers you have attached, the fewer alarm panels can be attached.

Store expiration date

If you want the badge expiration date to be used to determine the status of cards detected at the card readers, select “Date only” from the drop-down list. If the present date is later than the expiration date of the card, the card is considered to be invalid and access is denied.

If you do not want the badge expiration date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge expiration date and time to be used to determine the status of cards detected at readers. If the present date and time is later than the expiration date and time of the card, the card is considered to be invalid and access is denied.

Store activation date

If you want the badge activation date to be used to determine the status of cards detected at the card readers, select “Date only” from the drop-down list. If the present date is earlier than the activation date of the card, the card is considered invalid and access is denied.

If you do not want the badge activation date to be used to determine the status of card, select “Not enforced” from the drop-down list.

A third option, “Date and time” is available only if you selected the **Use time** check box on the General Cardholder Options form in the Cardholder Options folder. Select this option if you want the badge activation date and time to be used to determine the status of cards detected at readers. If the present date and time is earlier than the activation date and time of the card, the card is considered to be invalid and access is denied.

Timed anti-passback

Indicates that readers attached to this panel are to be used for timed anti-passback. You must also set the **Timed anti-passback setting (minutes)** field. This is done on the Anti-Passback form of the Readers folder.

Store area anti-passback location

Select this check box if a reader attached to this access panel is used to enter or leave an anti-passback area. Anti-passback areas are defined on the Anti-Passback Areas form of the Areas folder. The **Area entering** and **Area leaving** fields, located on the Anti-Passback form of the Readers folder, are used to associate specific readers with specific areas.

Precision access (reader inclusion)

If selected, it indicates that this access panel will use the application’s precision access capabilities. Precision access is a method for assigning unique access privileges to individual cardholders. There is an infinite number of precision access combinations that can be created and assigned to cardholders.

Note: Using this option severely limits the number of cardholders that can be stored in the panel. If you wish to use precision access, it is recommended that panel memory be expanded to meet your facility’s needs.

Elevator support

If selected, this panel will support elevator control. You must have at least 1 MB of memory to use this feature. This check box will be grayed out if 256 KB of memory is used.

First card unlock

If selected, this panel will have first card unlock functionality. First card unlock is used in conjunction with reader mode and timezone control. Doors configured with first card unlock will

not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.

Note: If the reader is in “Facility code only” mode, the first card unlock feature does not work.

Special area rules

When checked this option enables the Special Two-Man Rule. If this is the first time enabling this rule a check will be made on your system and a message displayed informing you that additional changes may have to be made to the cardholder badge options. For more information please refer to Appendix G: Special Two-Man Rule on page 1435.

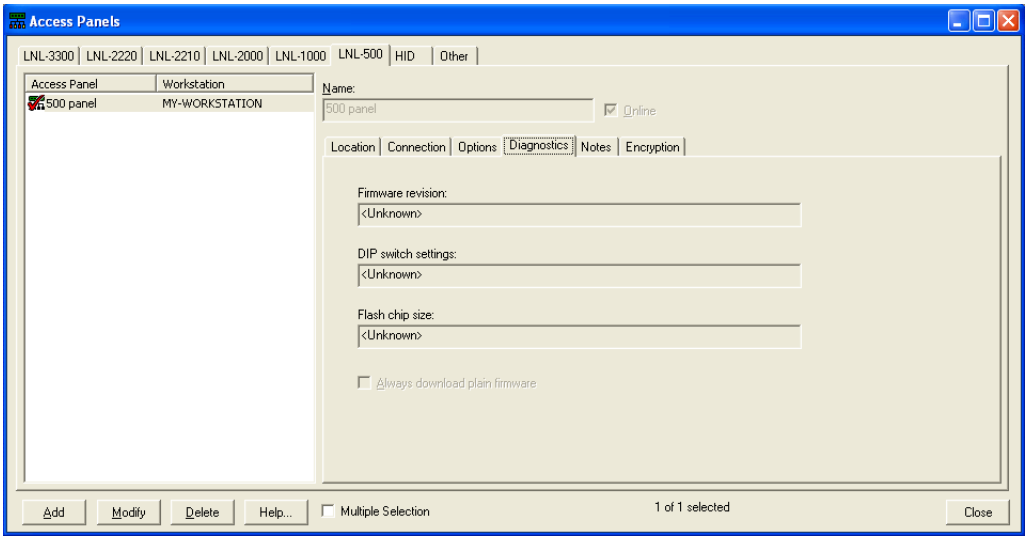
Event capacity

Calculates and displays the number of events that can be stored on the panel based on the parameters you’ve selected. The minimum is 1000 events. The memory usage in an access panel is based on two criteria:

- Memory used for cardholder storage
- Memory used for event history storage

After cardholder storage requirements are computed based on the options selected in this section, all remaining memory is used for event storage.

LNL-500 Form (Diagnostics Sub-tab)



Firmware revision

Displays the firmware revision reported by the controller the last time it was online. This is a read only text field.

DIP switch settings

Displays the DIP switch settings reported by the controller, the last time it was online. This is a read only text field. Note that DIP switch settings are read by the controller only when the

controller is powered up. DIP switch changes made afterward will not take affect until the controller goes through another power cycle.

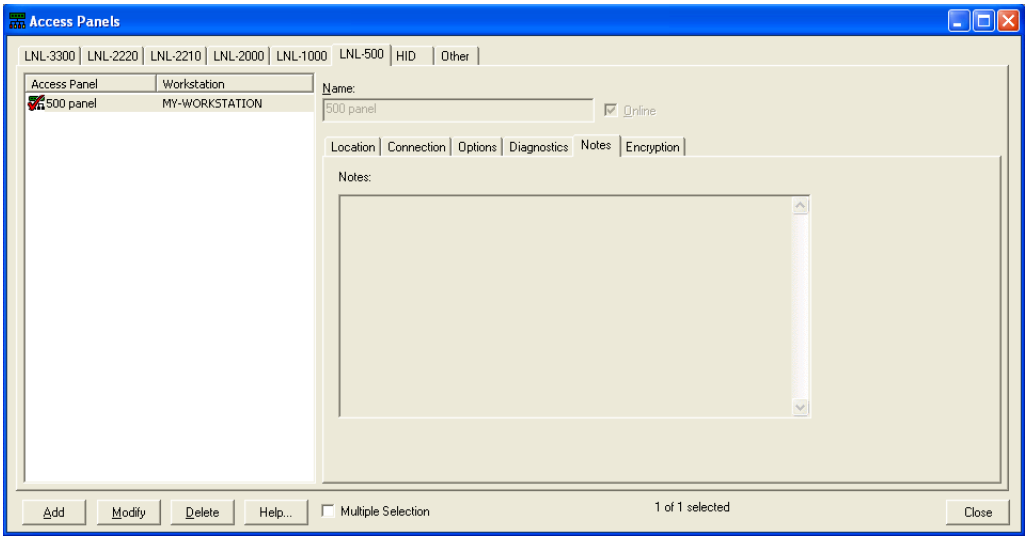
Flash chip size

Displays the flash chip size (128 KB or 256 KB) reported by the controller, the last time it was online. This is a read only text field.

Always download plain firmware

Determines the type of firmware downloaded to the controller. If not selected, (the default) the system downloads AES/Extended firmware to the controller whenever the controller has a 256 KB flash chip. If selected, the system always downloads plain firmware to the controller.

LNL-500 Form (Notes Sub-tab)



Notes

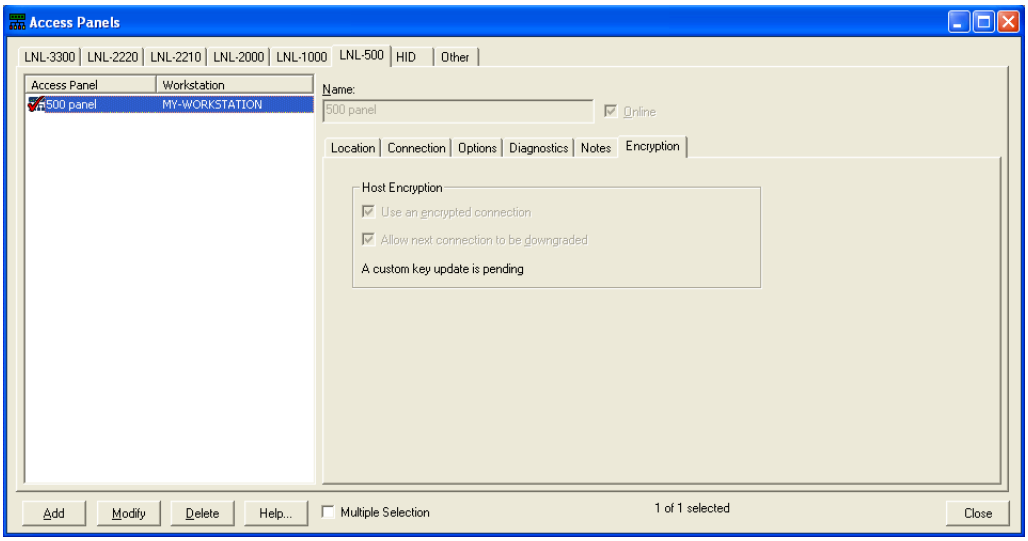
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

LNL-500 Form (Encryption Sub-tab)

This view displays when the system/segment (the panel is associated with) uses automatic encryption. When the system/segment is configured for manual encryption, the same fields display except for the **Allow next connection to be downgraded** check box.The Encryption sub-tab does not display if a system/segment uses a plain connection.

Note: The system/segment the controller belongs to must be configured for encryption in order for this tab to display. The user must also have the correct user permissions.

For more information about encryption, refer to the Encryption for Controllers User Guide.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key, the factory default master keys, and finally by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible. This check box displays only if the controller exists in an automatic key management system/segment.

A custom key update is pending

Indicates there is an outstanding key update for this controller. This is a read only field. This text field displays only if the controller exists in an automatic key management system/segment, and the condition exists (if there is an outstanding key update).

LNL-500 Form Procedures

Add an LNL-500 Access Panel

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** Menu. Click the LNL-500 tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the access panel.
4. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system or defining panels, but instead would wait until you're ready to put the panel into service.
5. Specify communication parameters on the Location and Connection sub-tabs.

6. Specify setup parameters on the Options sub-tab, which sets up the cardholder database for this panel.

   IMPORTANT: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

7. Click [OK].

Modify an LNL-500 Access Panel

Notes: Modifying the PIN type requires a full panel download.

If the PIN type is modified on the controller and/or the General Cardholder Options form, you must log off/log on to System Administration before you modify a cardholder pin number.

1. In the listing window, select the LNL-500 entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an LNL-500 Access Panel

1. In the listing window, select the LNL-500 entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enable an LNL-500 Access Panel for Encryption

The encryption modify/export permission is required to complete this procedure.

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu. Click the LNL-500 tab.
2. Click the Encryption sub-tab.
3. In the listing window, select the LNL-500 entry you wish to change.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the next connection to downgrade to a plain connection if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

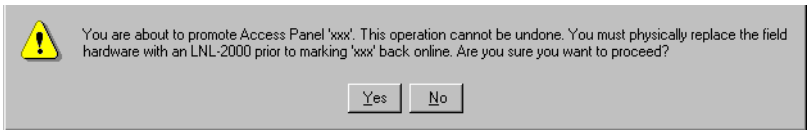
Promote an LNL-500 Access Panel to an LNL-1000, LNL-2000, LNL-2210, LNL-2220, or LNL-3300

Note: In order to promote an access panel, it must be offline.

In order to promote an access panel to an LNL-2210 the panel's Primary Connection must be configured as a LAN type. In addition, you may need to configure the panel so that it conforms to one of the configurations supported by the LNL-2210:

- Up to 8 downstream RS-485 devices (readers modules and alarm panels)
- Up to 17 readers (using 8 dual reader interface modules and 1 onboard reader).

1. In the listing window, right-click over the LNL-500 entry you wish to promote.
2. From the pop-up menu, select **Promote Access Panel to LNL-1000**, **Promote Access Panel to LNL-2000**, **Promote Access Panel to LNL-2210**, **Promote Access Panel to LNL-2220**, or **Promote Access Panel to LNL-3300**. The following message will be displayed:



3. Click [Yes] to continue.
4. Click [OK].

Enter Notes for an Access Panel

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

HID Form Overview

HID Edge access panels are IP devices that are treated as panels by OnGuard because they are able to contain a database that can operate autonomously from the OnGuard host.

Events from the HID panel are represented in Alarm Monitoring just as with any other traditional access control device. In Alarm Monitoring you can View Events (Door Forced and Door Held), Open Door, Manually Unlock (Free Access) Door, and Manually Lock (Lockdown) Door. Additionally, HID access panel events can be set to trigger Global I/O.

• WARNING! • The maximum number of cardholders (badges) that can be downloaded is 44,000 divided by the number of card formats specified for an HID panel. For example, 44,000/5 card formats = 8,800 badges while 44,000/1 card format = 44,000 badges. An alarm will be generated if the maximum number of cardholders is reached.

Note: Badge activate/deactivate dates will be adjusted to fall within acceptable ranges when badges are downloaded. Activate dates less than the minimum allowed are adjusted to 01/01/1970. Deactivate dates greater than the maximum allowed are adjusted to 12/31/2037.

IMPORTANT: HID supports a maximum of eight (8) access levels per badge. If more than 8 access levels with a common HID controller are assigned to a badge, only 8

access levels will be downloaded. In addition, other HID controllers in the same access level may be affected.

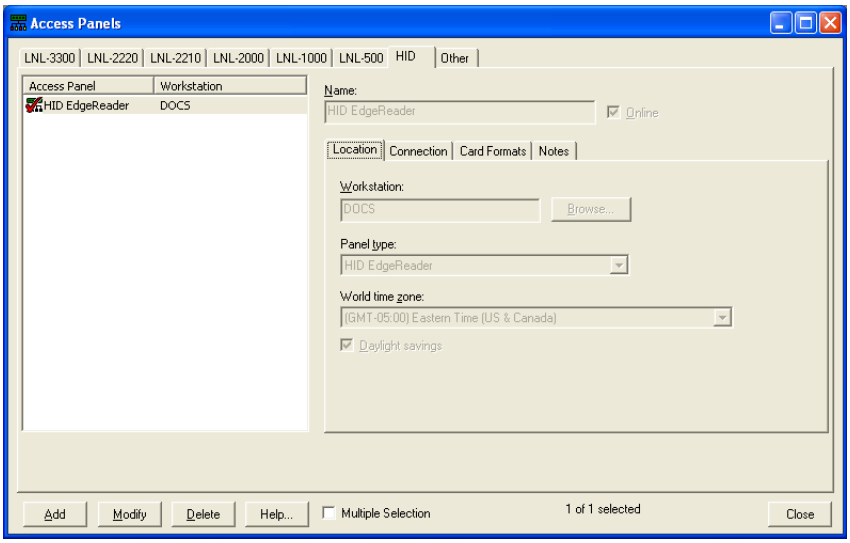
Supported HID panels include EdgePlus and EdgeReader. When either type of Edge panel is added, one (1) reader is automatically assigned to it.

Readers connected to HID panels can be used with OnGuard to provide basic access control functionality in locations where the full capability of Lenel access hardware is not needed.

Use the HID form to:

- Assign names to individual HID panels in the software.
- Specify HID panel setup parameters, including time zone and panel type.
- Specify the LAN communication panel setup parameters.
- Assign card formats to individual HID panels.

HID Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the HID panel type. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters. Though the name can be 32 characters it is advantageous to keep the name to 25 characters or less or else the reader name for the panel may be truncated.

Online

If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Selects the workstation or server to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation.

You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Note: You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

Panel Type

Select the type of HID panel you are adding. Choices include:

- HID EdgePlus - (HID EdgePlus only supports 8-bit keypad data).
- HID EdgeReader
- Lenel EdgePlus - (Lenel EdgePlus only supports 8-bit keypad data).
- Lenel EdgeReader

Note: Non-Lenel HID access panels require you to purchase a separate license. Lenel-branded HID access panels, however, come with a built-in license. Any combination of HID access panels can be added along with other types of access panels up to the maximum capacity of your OnGuard system. For more information, see the Licenses for Hardware section in the Installation Guide.

World time zone

Select the world time zone for the geographical location of the access panel. The options in the drop-down are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities located in that world time zone.

Daylight savings

Select this check box if Daylight Saving Time is enforced for the geographical location of the access panel.

Add

Adds a panel entry.

Modify

Changes a panel entry.

Delete

Removes a panel entry.

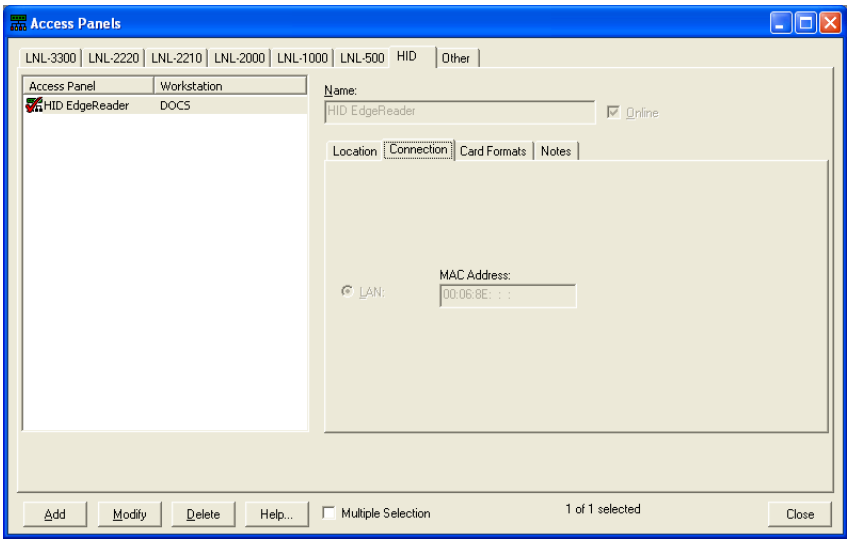
Help

Displays online help for this topic.

Close

Closes the Access Panels folder.

HID Form (Connection Sub-tab)



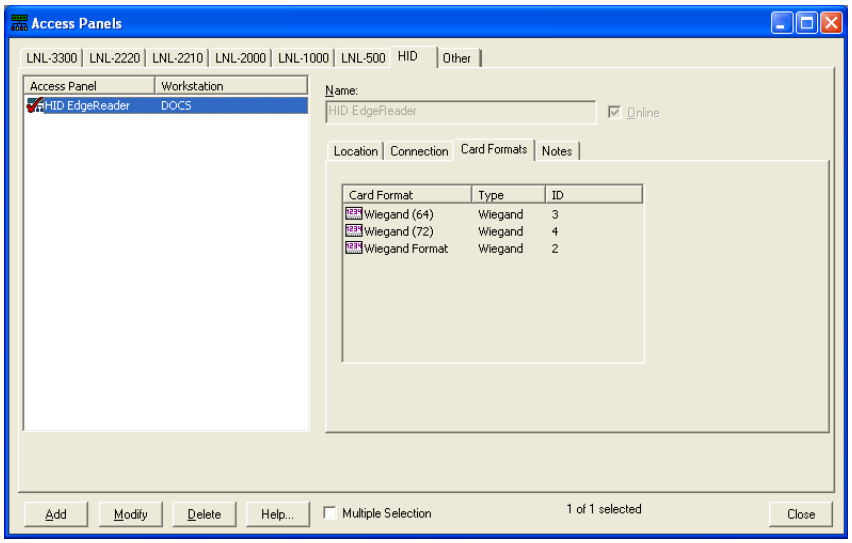
LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's **IP address**.

MAC Address

If you selected the **LAN** radio button, enter here the MAC address for the access panel, as listed on the device.The access panel itself must be configured to have the same MAC address that is entered in this field.

HID Form (Card Formats Sub-tab)



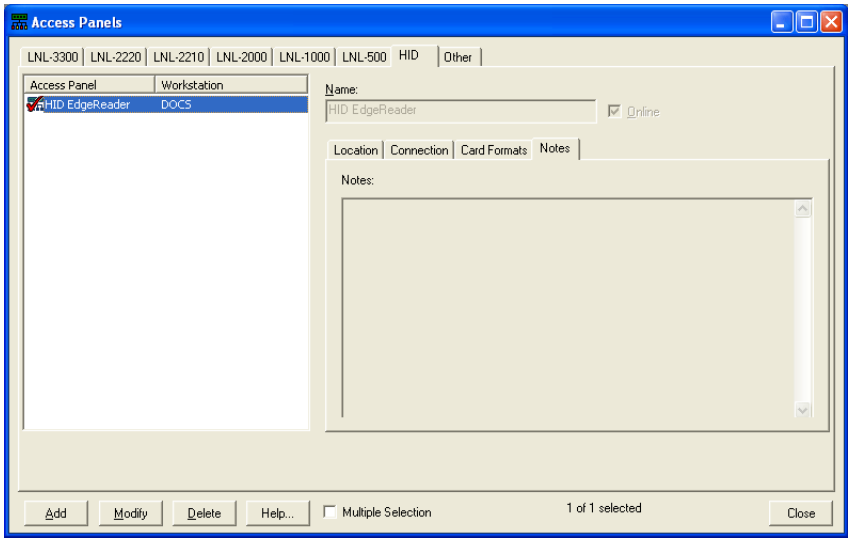
Card Format

Identify the format(s) expected when a card is presented to an HID reader. Card formats are defined in the Card Formats folder.

HID panels are limited to using Wiegand format cards with no more than 128 bits and with "HID Corporate 1000" or "None" selected in the **Special** setting of the card format. For more information, refer to Wiegand Card Format Form on page 252.

Card formats specified for an HID access panel are applied to all readers assigned to that panel.

HID Form (Notes Sub-tab)



Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

HID Form Procedures

The following procedures can be performed on this form.

Add an HID Access Panel

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu. Click the HID tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the access panel.
4. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn’t check this box when configuring the system or defining panels, but instead would wait until you are ready to put the panel into service.
5. Specify the communication parameters on the Location and Connection sub-tabs.
   - The MAC address you enter on the Connection sub-tab can be found on the HID reader itself.
6. Select one or more card formats on the Card Formats sub-tab.

   IMPORTANT: These access panel settings must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.
7. Click [OK].

Modify an HID Access Panel

1. In the listing window, select the HID entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an HID Access Panel

1. In the listing window, select the HID entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enter Notes for an HID Access Panel

1. In the listing window, select the entry you want to edit.
2. Click [Modify].

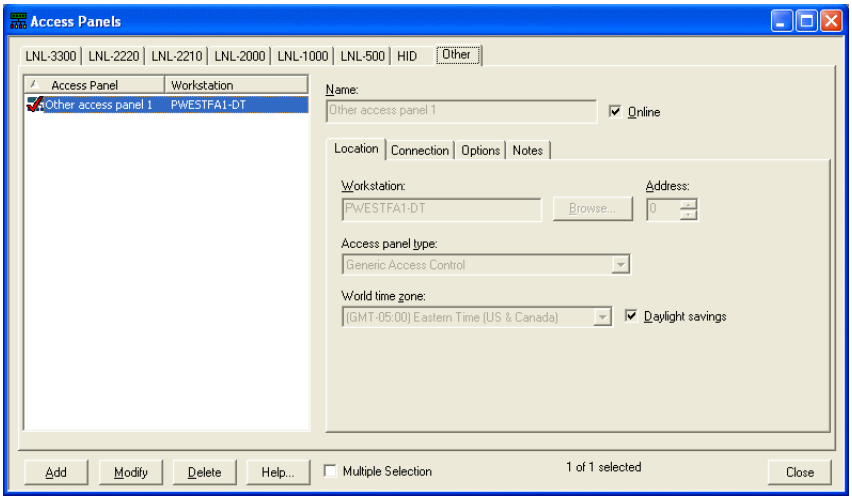
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Other Form Overview

This form is used to:

- Assign names to generic type access panels in the software. Mainly used to support additional access control type panels that may be integrated via the OpenAccess Alliance Program.
- Specify access panel setup parameters.
- Specify communication panel setup parameters, including the workstation associated with the panel

Other Form (Location Sub-tab)



Workstation

Selects the workstation or server to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Note: You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer window, from which you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field on the Other form.

Address

Specifies the panel's address, which will match the DIP switch setting on the panel itself. Each panel must have a different address. Possible values are in the range of 0 through 7. The factory default DIP switch setting is 0.

Access panel type

Select the type of access panel you are adding.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Add

Adds a panel entry.

Modify

Changes a panel entry.

Delete

Removes a panel entry.

Help

Displays online help for this topic.

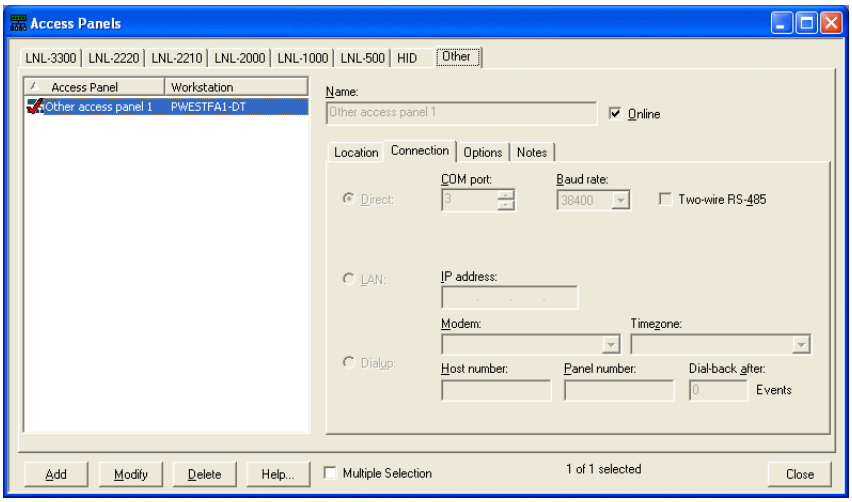
Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected panels.

Close

Closes the Access Panels folder.

Other Form (Connection Sub-tab)



Direct

Select this radio button if communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**, the **Baud rate**, and whether or not communication to the host will use a **Two-wire RS-485** connection.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 through 255.

Baud rate

If you selected the **Direct** radio button, this is the speed (in bits per second) at which information is transferred between the workstation and the access panel via the serial connection.

Note: Some third party devices do not allow the baud rate to be modified from the host application software. If such a device is in use, the baud rate setting in OnGuard has no bearing. Refer to the documentation for any third party devices being used.

Two-wire RS-485

The panel can be configured to communicate with the host workstation using either a 4-wire or 2-wire RS-485 connection. Select this check box if 2-wire communication is to be used.

LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's **IP address**.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Dialup

Select this radio button if the workstation will communicate with the access panel using a dialup connection. This option functions together with the **LAN** option on the Secondary Connection sub-tab to limit combinations of primary and secondary communications for dual path usage.

You must also specify the workstation's **Modem**, **Timezone**, **Host number**, **Panel number** and **Dial-back after__Events**.

Modem

If you selected the **Dialup** radio button, select the modem on the workstation that will be used for dialup communication with the access panel. Choices include all TAPI (Telephone Application Programming Interface) devices that are currently configured on the specified **Workstation**.

Before a modem can be listed in this drop-down list, the modem must be properly configured for the selected **Workstation**. This is done on the Modems form in the Dialup Configuration folder, which is reached by selecting ***Modems*** from the ***Access Control*** menu. For more information, refer to Connect a Modem to a Lenel Access Panel on page 704. If any of the TAPI devices are used for other dial functions such as remote access, do not select them for panel dial usage. For more information, refer to your Windows user guide.

Timezone

If you selected the **Dialup** radio button, indicate the timezone during which the access panel will initiate dialup communication with the workstation. You can select only one timezone for the particular workstation-modem-panel combination. Timezones are defined on the Timezones form of the Timezones folder.

Host number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the workstation. This is the number that the access panel will use to dial into the panel to send events and other transactions to the workstation. Type the exact dialing sequence here. Although you can use parentheses and dashes, they are ignored by TAPI devices. For example, 2489720 and (212) 546-1234. For more information, refer to your Windows user guide.

Panel number

If you selected the **Dialup** radio button, enter the phone number used to reach the modem that's connected to the access panel. This is the number that the workstation would need to dial to communicate with the access panel.

Typically, all communication between the access panel and the workstation is initiated from the panel. However, the workstation can dial the panel from within the Alarm Monitoring system. This is done by right-clicking on the panel's entry in the System Tree, then selecting the **Connect** command from the popup menu. Any ASCII string can be typed here (for example, a comma typically triggers a pause in the dialing sequence).

Dial-back after__Events

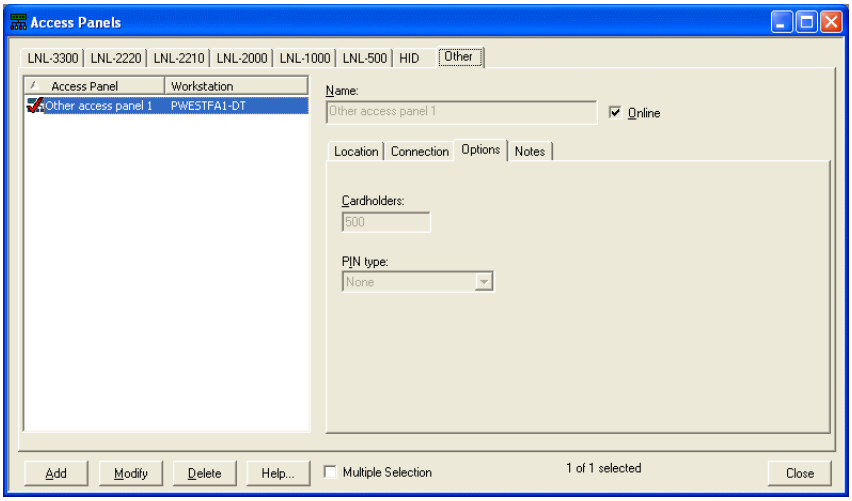
This field is displayed only if you have selected the **Dialup** radio button.

Panels can be programmed to dial the workstation after a certain number of events have been stored in the panel but have not yet been reported to the host (because the panel has been offline).

When the panel has accumulated the specified number of stored events, the panel will automatically dial the **Host Number** to dump its transactions and to receive any command programming. After the information has been exchanged, the workstation will terminate the connection.

The default value here is 255 events. The minimum value you can enter is zero (meaning that the panel will never dial the host). The maximum value is equal to one less than the maximum number of events that the panel can store.

Other Form (Options Sub-tab)



PIN type

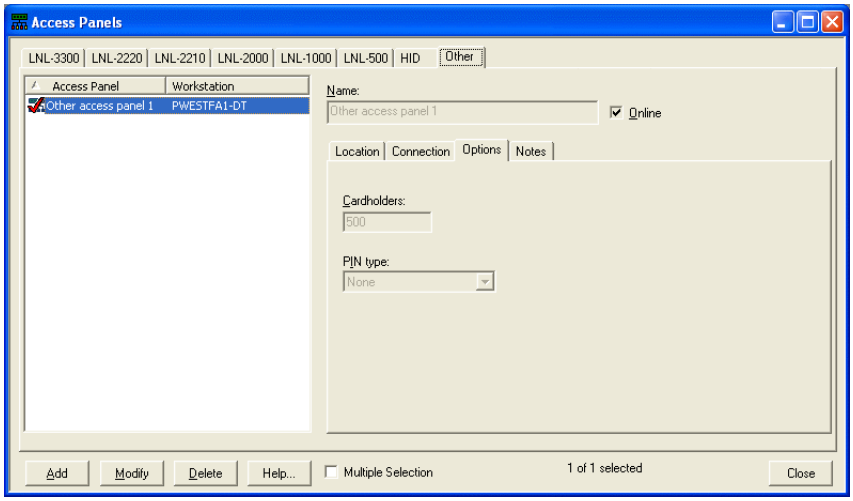
Select the range of PIN digits allowed. Using PINs takes up memory on the access panel, which reduces the card capacity.

If you have a pin code configured for a controller that is 1-n digits long, but have a cardholder in the database that has a pin code longer than n, the pin code gets downloaded with the badge record, but gets truncated at n digits. For example, you have a 1-4 digit pin for the controller, but the badge record in the access control system's database has '123456' specified as the pin code. When this gets downloaded, it is truncated to '1234.' The Cardholder can either enter the first 4 digits or all 6 digits correctly and gain access.

Cardholders

This field determines how much of the access panel's memory will be set aside for the cardholder records. This size is limited by the size of the access panel's memory, and is directly related to the options you choose in this section. The more options you choose and the more that each option requires (more digits in the card number, for example), the fewer the maximum number of cardholders possible.

Other Form (Notes Sub-tab)



Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

Other Form Procedures

The following procedures can be performed on this form.

Add an Other Access Panel

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for the access panel.
3. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn’t check this box when configuring the system or defining panels, but instead would wait until you’re ready to put the panel into service.
4. Specify communication parameters on the Location and Connection sub-tabs.
5. Specify setup parameters on the Options sub-tab, which sets up the cardholder database for this panel.

   IMPORTANT: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

6. Click [OK].

Modify an Other Access Panel

1. In the listing window, select the Other entry you wish to change.
2. Click [Modify].

3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an Other Access Panel

1. In the listing window, select the Other entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enter Notes for an Access Panel

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Threshold Settings in the ACS.INI File for Dialup Panels

IMPORTANT: Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

Additional threshold settings can be configured for Lenel dialup panels by modifying the **ACS.INI** file. The **ACS.INI** file is located in the Windows directory of the workstation to which the dialup panel will be connected. The following are options that are located in the [Service] section of the **ACS.INI** file

[Service]	Description
FailedRPCLowWaterMark=0	• Determines if a dialup panel needs to be called if the number of failed RPCs reaches a specified threshold • FailedRPCLowWaterMark is set to 0 (off) by default, which means that it is not enabled. • FailedRPCLowWaterMark can be enabled and set to a number that serves as the threshold for the number of failed RPCs for a specific dialup panel. For example: • FailedRPCLowWaterMark=50
LastDialupConnectionCheck=0	• Checks when the last connection to a specific dialup panel occurred. If too many hours have elapsed, a call is initiated to the panel. • LastDialupConnectionCheck is set to 0 (off) by default, which means that it is not enabled. • LastDialupConnectionCheck can be enabled and set to a number that serves as the threshold for the number of hours since the dialup panel has called. For example: • LastDialupConnectionCheck=10

[Service]	Description
LogEventThread FilePath=C:\acce ssct[PW1]\	• Allows the Communication Server to save events to a file upon shutdown that it was unable to save to the database • The file that these events are saved to is called LogEventThreadEvents.dat • The default location where the LogEventThreadEvents.dat file is saved is the current directory that the Communication Server is run from • Another location can be chosen by setting the LogEventThreadFilePath to a different path. For example: • LogEventThreadFilePath=C:\tmp\

If FailedRPCLowWaterMark is set to any value other than 0, the Communication Server will check the number of failed RPCs for non-connected dialup panels approximately once an hour. If the number of failed RPCs in the database is greater than the specified threshold number, a connection to the panel is attempted.

- When this connection attempt occurs, an alarm is displayed in the Alarm Monitoring application that reads “Dialup Stored Command Limit Exceeded”.
- No status indication of the actual connection and processing of failed RPCs is indicated in the alarm.

The purpose of the LastDialupConnectionCheck option in the ACS.INI file is to identify panels that have not connected, but should have. This helps identify panels in the field that are damaged or are experiencing problems. If LastDialupConnectionCheck is set to any value other than 0, the Communication Server will check the most recent connection time for each dialup panel approximately once an hour. Only panels that have connected at least once (since this build has been installed) will be checked. If the amount of time that has elapsed since the dialup panel last connected is greater than the specified threshold number, a connection to the panel is attempted.

- When this connection attempt occurs, an alarm is displayed in the Alarm Monitoring application that reads “Dialup Last Connection Time Expired”.
- No indication of whether the connection was successful or not is indicated.

LogEventThreadFilePath allows you to save events to a file upon shutdown that it was unable to save to the database. Normally, this should not occur. This should only occur if there was a problem writing to the database. When the Communication Server is started, it checks to see if the LogEventThreadEvents.dat file exists using the path specified in the ACS.INI file. If the file does exist, the Communication Server will read the events that are in the file, save them to the database, and delete the file.

If the Communication Server gets into a state where it can still open the database but is having problems writing to the table that the events are stored in, the Communication Server will stop polling the panel for events until it can write another event to the database. Error messages will be recorded in the following locations:

- “Database Error” messages will be sent to Alarm Monitoring as a warning that this condition occurred
- Application Log
- LenelError.log

The information contained in the error messages is useful in determining exactly why the Communication Server was unable to write to the database. The Communication Server will probably need to be shut down to get the system to work properly.

- Shutting down the Communication Server will save any unsaved events to the LogEventThreadEvents.dat file.
- When the Communication Server restarts, it will load the events from the LogEventThreadEvents.dat file and attempt to save them to the database. (The events will not be sent to Alarm Monitoring because they were already sent once.)
- Before restarting the database, the error logs should be examined and any problems with the database should be resolved.

CHAPTER 28

Readers and Doors Folder

The Reader folder contains forms with which you can:

- Name individual readers in the software
- Identify the reader's type and its access panel address
- Specify reader setup parameters, including access panel connection, and modes of operation

The folder contains the following forms: the General form, the Grouping form, the Settings form, the Controls form, the Aux Inputs form, the Aux Outputs form, the Anti-Passback form, the Command Programming form, the Elevator Hardware form, the Door form, the In Reader form, and the Out Reader form, the ILS form, and the ILS Priority One Events form.

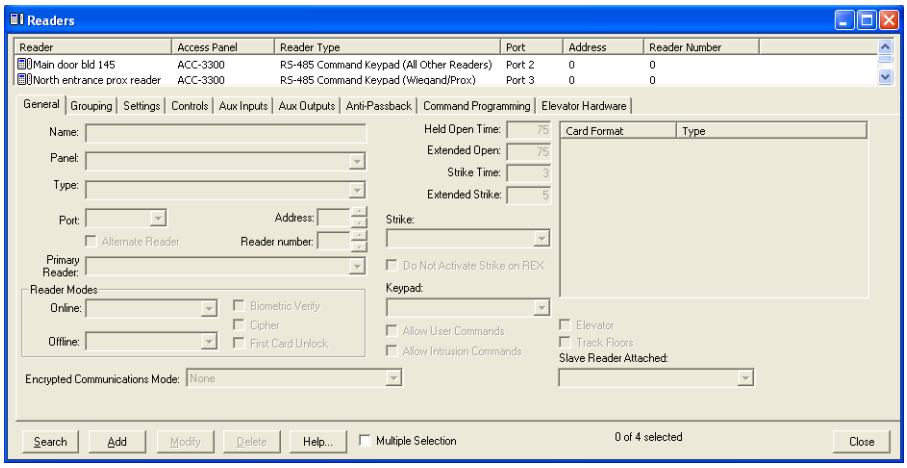
The Readers folder is displayed by selecting ***Readers and Doors*** from the ***Access Control*** menu, or by selecting the Readers and Doors toolbar button.

Toolbar Shortcut

General Form

The General form is used to:

- Name individual readers in the software
- Identify the reader's type and its access panel address
- Specify offline and online modes of operation, and the card format used



Note: Reader functions supported for HID panels allow you to grant access on “Card Only” or “Card and Pin” and configure strike time, held time, and extended strike for specified users. Additionally, strike on REX can be disabled/enabled. For more information, refer to the HID Form Overview on page 620.

Listing window

Lists currently defined readers, the access panel to which each is connected, and each reader’s type. It also lists the reader’s port, address, and reader number.

Name

Enter a unique reader name of no more than 32 characters. The application uses the name when assigning card readers to access groups, when monitoring alarms, and elsewhere in the system.

Panel

Select the access panel to which the reader is attached. Choices include all currently defined access panels.

Type

Select the type of reader that is being configured. Available choices depend upon the type of access panel that the reader is connected to.

Note: On-board reader #1 must be configured as the master of the pair and on-board reader #2 as the slave. For more information, refer to Settings Form on page 645.

Note: The LNL-2210 panel supports two different configurations. The first allows you to add up to 2 on-board readers to the panel. However, on-board reader #2 cannot be added if the panel already has downstream devices associated with it. The second configuration allows you to add up to 8 downstream devices (off-board readers or alarm panels) or up to 16 off-board readers to the panel. However, you cannot add a second on-board reader.

IMPORTANT: A full panel download may be required the first time a downstream device (off-board reader) is added to an LNL-2210 panel or when the only downstream device assigned to that panel is deleted.

Port

Select the port on the access panel that the reader board attaches to. Different access panels have a different number of communication ports that connect to devices such as reader boards and alarm panels. Dual readers use the same port.

Note: "Reader 1" must be used as the port for off-board readers attached to the LNL-2210.

Address

Select the address that was set on the reader board during installation. The reader board address is set using DIP switches. Addresses range from 0 - 31.The address you enter in System Administration must match the reader board address.

Exceptions:

- Dual readers - Dual reader #1 must use the LNL-1320 address. Dual reader #2 can use a different address. It is recommended that you use the same address to free up an address for a different device.
- Gateway readers - must use the address that was set on the gateway board (i.e.LNL-500B). This applies to every biometric reader connected to the same gateway board.

Note: Readers are differentiated by their reader number.

Alternate Reader

Select this check box if you want an alternate reader associated with a primary reader. Alternate readers can be either a biometric or generic reader.

Requirements for Biometric Reader Support

- Biometric readers must be alternate readers. Therefore, this check box must be selected when you configure a biometric reader.
- The **Biometric Verify** check box (located on the General form) must be selected when you configure the Primary reader.

About Generic Alternate Reader Support

- A generic alternate reader is a secondary read head and/or keypad that works with a primary reader. Together the generic alternate reader and the primary reader function as one logical reader.
- The REX, Strike, and Door Contact come from the primary reader's interface.
- All access related events are considered events for the primary reader.

Reader number

The reader number differentiates readers that use the same port and address. Values typically range from 0 - 7. However, for the following readers:

- Scaled Wireless Access readers - The reader accepts reader numbers from 0 - 15.
- Dual readers - The reader number is a fixed value that you cannot change.
- Gateway readers - The first reader must be reader number 0. The second reader can be any number.

The reader number is related to the gateway reader address/node number. For example with HandKey readers, reader number 0 on the gateway corresponds to the HandKey reader with address 0 and reader number 5 corresponds to the HandKey reader with address 5. A similar thing is done with Bioscrypt and Scaled Wireless Access.

Primary Reader

If you are configuring an alternate reader, select the primary reader associated it.

Online (Reader mode)

Specify the reader's mode when it's online and communicating with the access panel. Most of the modes are self explanatory, except for **Facility Code Only** mode, which means the access grant decision is based on the cardholder's facility code setting.

When using PIN only access (PIN or Card mode) at a reader configured for Biometric verification, PIN configurations should be unique. Otherwise, two cardholders having the same PIN may be denied access due to the wrong biometric template in the database being used for verification.

Choosing a PIN only access (by selecting the Pin or Card option) is not recommended because it provides a low level of security.

Offline (reader mode)

Specify how the reader behaves when communication is lost between the reader and the access panel (if the reader is wired to the access panel), or between the reader and the intelligent reader. Applicable choices depend upon the type of reader. All readers with the exception of downloadable readers can only choose from locked, unlocked or facility code as valid offline modes of operation.

When using PIN only access (PIN or Card mode) at a reader configured for Biometric verification, PIN configurations should be unique. Otherwise, two cardholders having the same PIN may be denied access due to the wrong biometric template in the database being used for verification.

Choosing a PIN only access (by selecting the Pin or Card option) is not recommended because it provides a low level of security.

Biometric Verify

Select this check box if the primary reader is used along with a biometric reader. The primary reader will ask for verification from the alternate (biometric) reader only if this check box is selected.

This field can be used in conjunction with the verify mode fields, on the Timezones folder, if you want biometric verify mode based on timezones. To display the Timezones folder, select ***Timezones*** from the ***Access Control*** menu, and select the Timezone/Reader Modes form.

Cipher

Lenel hardware only - Select this check box if you want cipher mode enabled for the reader. When a reader is in cipher mode, card data can be entered via the keypad.

In addition to selecting this check box, a magnetic card format must be assigned to the reader (even for Wiegand readers). When set, a keypad sequence starting with “*” and ending with “#” will be treated as a magnetic card read stream and matched against the formats assigned to the reader.

First Card Unlock

First card unlock mode is only supported on Lenel controllers. However, first unlock behavior can be configured for use with any controller through global I/O support. Note that whenever a reader’s mode is changed, the first card unlock mode is automatically disabled.

Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode changes to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.

This field is used in conjunction with the **First Card Unlock** check box on the Timezone/Reader Modes form in the Timezones folder. This is so that timezone control can be used to specify when the reader uses the first card unlock functionality. If the reader is in “Facility code only” mode, the first card unlock feature does not work.

Encrypted Communications Mode

This field is used for configuring downstream encryption. The options are:

- **None** - encryption is not required to send communication.
- **Not Required** - encryption is attempted but if it fails the communication is sent unencrypted.
- **Required** - encryption is attempted but if it fails the communication is not sent.
- **Custom** - the custom key is used and if communication cannot be established then an encryption error status is generated.

This field is enabled only if the following conditions are met:

- The panel type is an LNL-1100 or LNL-1200.
- The reader is connected to an LNL-2220 or LNL-3300 access panel.
- Host and downstream encryption are both enabled for the specific access panel.

Held Open Time

Specify the number of seconds the door can be held open before an alarm generates.

- Lenel hardware - Enter a value from 1 to 131,070 seconds (36.4 hours).
- Other types of hardware - Enter a value from 1 to 255 seconds (4.25 minutes).

Extended Open

Lenel hardware only - Specify the held open time for badges with the extended strike/held times feature enabled (on the Badge form of the Cardholders folder).This field is intended for anyone who needs extra time to proceed through a doorway. Values range from 1 - 131,070 seconds (36.4 hours).

Strike Time

Specify the number of seconds a strike or lock is open (activated) when access is granted. Typically, this is set from 5 - 10 seconds, but you can enter a value from 1 - 255 seconds (4.25 minutes).

If you are using Scaled Wireless Access readers, the strike time value should be set to the value matching what is set in the Scaled Wireless Access reader itself. You can not change the strike time via System Administration. This can only be done though the Scaled Wireless Access reader itself.

Extended Strike

Lenel hardware only - Specify the reader strike time for badges with the extended strike/held times feature enabled, on the Badge form of the Cardholders folder. This field is intended for anyone who needs extra time to proceed through a doorway. Values range from 1 - 255 seconds (4.25 minutes).

Strike

For Lenel panels - Indicates how the door strike behaves when a valid card swipe occurs. Choices include:

- **Cut Off on Close** - cuts off the door strike when the door closes. This is the default setting.
- **Cut Off on Open** - cuts off the door strike when the door opens.

Do Not Activate Strike on REX

For Lenel panels - A *REX (Request to Exit) contact* is typically a button located near the associated door. When a cardholder pushes the button a REX is sent to the panel. If this check box is selected, the door strike will NOT energize when the REX contact closes. If this check box is not selected, the door strike energizes when the REX closes.

Keypad

Choose the type of keypad (if any) this reader has.

Allow User Commands

Select this check box if you are configuring a command reader. A *command reader* is equipped with a keypad by which system functions are performed. This check box must be selected before you specify the actions triggered by the keypad entries. Actions are specified using the Command Programming form of this folder.

Allow Intrusion command

Select this check box if you want the reader to have the intrusion command authority enabled. While this setting is available on all Lenel readers that are not elevator readers this should only be used for the LNL-CK reader, which has proper displays for the intrusion command.

Card Format

Identify the format(s) expected when a card is presented to a reader. Card formats are defined in the Card Formats folder. The system has the flexibility to incorporate multiple technologies from different readers. For example, a master reader might use a magnetic format, while the associated slave reader might use Wiegand Format. If the panel is an LNL-1000, you can select multiple card formats for a single reader.

Multiple Selection - During multiple selections, the card format list is disabled unless the selected readers are of the same type or are Lenel readers.

Sorting - Click on the Card Format column to sort the card formats.

Note: Card formats for HID readers are automatically specified based on the card formats selected for the panel to which the reader is assigned and cannot be modified on the General form. For more information, refer to HID Form (Card Formats Sub-tab) on page 624.

Elevator

Lenel readers - Select this check box you are configuring an elevator reader. Elevator control is supported through reader 1 on the dual reader interface board (LNL-1320). This check box can be selected only if you select one of the “Dual Interface Rdr 1” choices in the **Type** field on this form. This check box must be selected before you can further configure elevator access via the Elevator Control form on the Access Levels folder.

Track Floors

Select this check box ONLY if you intend to install alarm input modules.To use the floor tracking feature, you must also define the input and output panels using the Elevator Hardware form, and the outputs themselves using the Alarm Outputs form. For more information, refer to Elevator Hardware Form on page 672.

Single interface readers on Lenel panels - Select this check box to enable cardholder tracking with respect to the floors they access. When floor tracking is enabled, and a cardholder in an elevator cab selects one of the floor buttons, an alarm monitoring transaction is generated that identifies the cardholder and indicates which button was pressed. If the cardholder does not have access to the requested floor, an Access Denied event is generated.

Dual Interface Reader 2

Lenel panels with dual readers only - Specify the name of the second reader. The second reader must have been previously defined on this form and “Dual Interface Rdr 2” must have been selected as the reader **type** when you defined the second reader. If the primary reader is a Lenel elevator reader, this field is not supported.

Add
Adds a reader to the system.

Modify
Changes a reader entry.

Delete
Removes the selected reader(s).

Help
Displays pertinent help information onscreen.

Multiple Selection
If selected, two or more reader entries can be simultaneously checked in the listing window.

Close
Closes the Readers folder.

Hardware Notes

OnGuard supports two keypad command readers, the LNL-CK in RS-485 connection mode and the LNL-CK in LNL-1320 connection mode. OnGuard also supports the LNL-1300T, which is a discontinued keypad command device.

For more information, refer to the Command Keypad section of the Hardware Installation Guide.

LNL-CK in RS-485 Connection Mode

The LNL-CK in RS-485 connection mode is a device with a keypad and display that connects directly to a RS-485 line. This device has no inputs or outputs therefore, this device has no door strike, door contact, or REX functionality.

Note: If you want door inputs and door outputs, use the LNL-CK in RS-485 connection mode as an alternate reader and use the read head, door inputs, and door outputs of an associated primary reader.

The LNL-CK in RS-485 connection mode supports PIN only verification. However, you can wire a card reader into the unit so that card entry as well as pin only verification can occur.

LNL-CK in LNL-1320 Connection Mode

The LNL-CK in LNL-1320 connection mode is a device with a keypad and display that can connect to a reader port on an LNL-1320. An actual card reader can also be wired into the LNL-CK module. This device provides a keypad, LCD, card reader, and door inputs/outputs in single logical unit.

The LNL-CK in LNL-1320 connection mode supports PIN or Card verification.

LNL-CK Reader Types

Refer to the following reader type definitions to configure LNL-CK readers.

- RS-485 Command Keypad (LNL-1300T) - denotes an LNL-1300T connected to the RS-485 line. The LNL-1300T has been discontinued.
- RS-485 Command Keypad (All Other Readers) - denotes an LNL-CK connected to the RS-485 line. The card reader attached to the LNL-CK is an “all other readers” type.

- RS-485 Command Keypad (Wiegand/Prox) - denotes an LNL-CK connected to the RS-485 line. The card reader attached to the LNL-CK is a “Wiegand/Prox” type.
- RS-485 Command Keypad (Mag w/ Wiegand Output) - denotes an LNL-CK connected to the RS-485 line. The card reader attached to the LNL-CK is a Mag w/ Wiegand Output type.

General Form Procedures

Use the following procedures on this form.

Add a Reader

IMPORTANT: If you want to configure (add) several readers or ILS offline/wireless locks, use the Configure Readers Wizard which is available by selecting ***Wizards*** from the ***Application*** menu. The wizard provides detailed instructions to guide you through the configuration process. The wizard cannot be used to add biometric or Schlage wireless readers.

The mandatory fields required to add a reader include: **Name**, **Panel**, **Type**, **Port**, **Address**, **Reader modes** (online and offline) and associated **Card Format**. Other fields may be required depending on the type of system and hardware you are using.

Notes: If you are adding a reader for a V1000 access panel, the mandatory fields include: **Name**, **Panel**, **Type**, **Port** (1/2, 3/4), and **Address** (0 - 15).

For all other HID panel types, readers are automatically created; one (1) reader for each Edge panel, and two (2) readers for each V2000 panel. For more information, refer to HID Form Overview on page 620.

The following procedures include the required fields for a basic system. Refer to General Form on page 635 for information on additional fields.

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. On the General tab, click [Add].
3. In the **Name** field, enter a unique, descriptive name for the reader.
4. In the **Panel** drop-down, select the access panel the reader connects to.
5. Select the reader’s type. Keypad command reader type definitions are available in LNL-CK Reader Types on page 641.
6. Choose the port and address that connects the reader to the access panel.
7. Select one or more card formats.
8. Select the mode the reader should be in when the panel is online and offline.

Note: When using PIN only access (PIN or Card mode) at a reader configured for Biometric verification, PIN configurations should be unique. Otherwise, two cardholders having the same PIN may be denied access due to the wrong biometric template in the database being used for verification.

9. Click [OK].

Modify a Reader

1. On the General form, select (place a check mark beside) the reader entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes or [Cancel] to revert to the previously saved values.

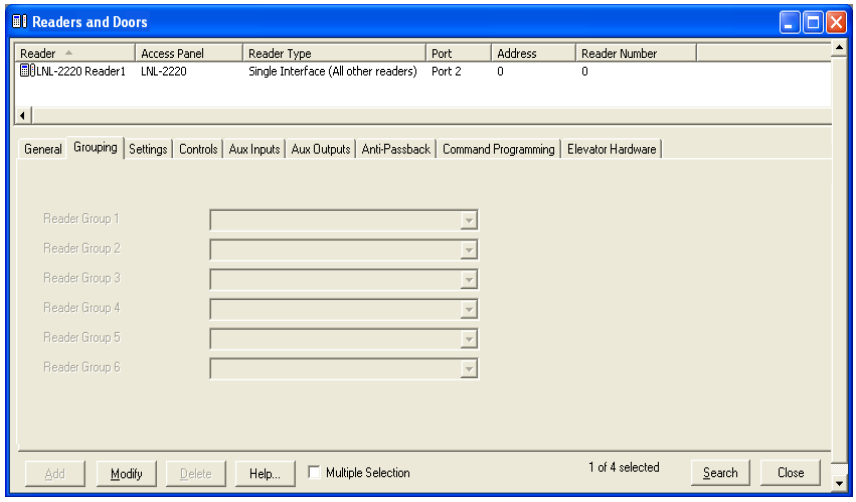
Delete a Reader

1. On the General form, select (place a check mark beside) the reader entry you wish to delete.
2. Click [Delete].
3. Click [OK].
4. Click [OK] to confirm deletion.

Grouping Form

The Grouping form is used to:

- Specify the group or groups to which the reader belongs.
- Search for readers by group (The search for readers button is available from all of the forms in the Readers folder.)
- Name and save lock group search criteria for future use.
- Six (6) default reader group drop-down lists are provided on this form.



Reader Group List Entries

In order to activate the reader group features, you need to add entries to each of the group lists you are planning to use in List Builder.

Reader Group Labels

Use FormsDesigner Lite to modify the label text (such as “Reader Group 1”) to better describe how you want to refer to the reader groups for your system.

Note: If you have the full version of FormsDesigner, in addition to modifying the label text, you can add reader group drop-down lists to the form and modify the default reader group lists. For more information, refer to the FormsDesigner User Guide.

Grouping Form Fields

Listing window
Lists currently defined readers (locks), the controller panel to which each is connected, and each lock's type. It also lists the lock's ID (Reader number).

Reader Groups
Specify groups for the selected reader (lock) from the **Reader Group** drop-down lists. Choices include the reader (lock) group values that were added in the List Builder folder.

Search
Displayed in view mode on every form in the Readers folder. This button is used to search for and list existing readers (locks) that meet the specified lock group search criteria.

Modify
Allows you to change reader (lock) group entries.

Help
Displays pertinent help information.

Multiple Selection
If selected, two or more reader (lock) entries can be simultaneously selected in the listing window.

Close
Closes the Readers folder.

Grouping Form Procedures

Use the following procedures on this form.

Add Reader Groups

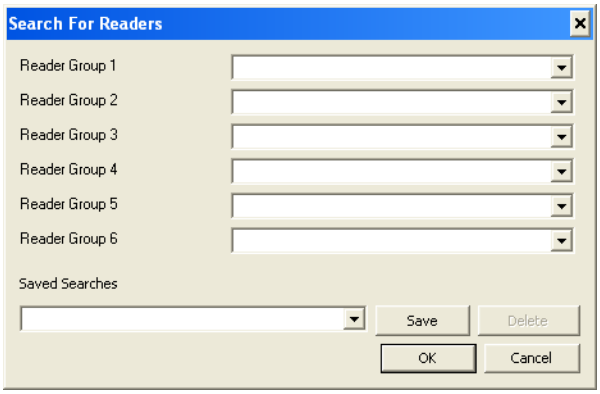
In System Administration, complete the following steps:

1. Select ***Readers*** from the ***Access Control*** menu. The Readers folder opens.
2. From the readers list, select the reader you want to configure.
3. Click [Modify].
4. From one or more of the **Reader Group** drop-downs, select a group item to assign to the lock.
5. Click [OK].

Search for Readers by Groups

In System Administration, complete the following steps:

1. Select ***Readers*** from the ***Access Control*** menu. The Readers folder opens.
2. In view mode, click [Search]. The Search for Readers window opens.

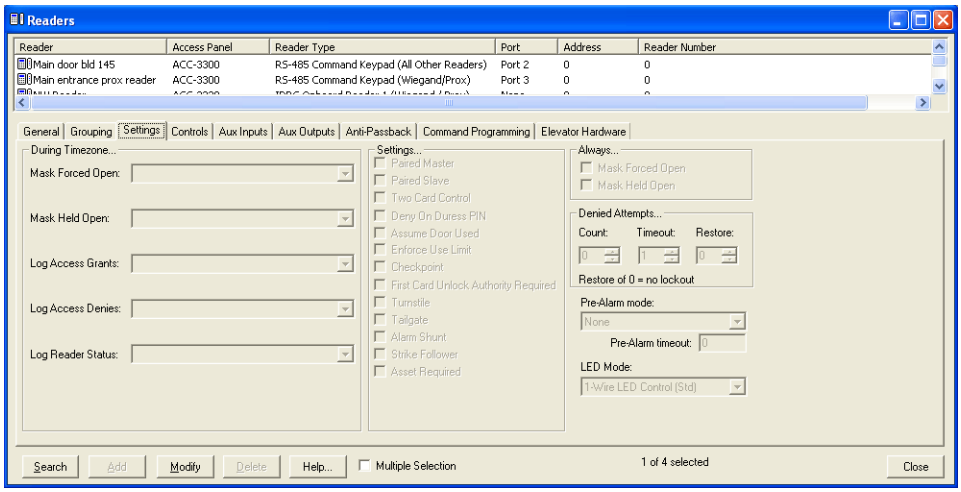


3. Specify your search criteria by selecting entries from one or more of the **Reader Group** drop-downs.
4. (Optional) Type a unique, descriptive name for the current search criteria, and then click [Save] to save the search settings. To remove a saved search, select the search name in **Saved Searches**, and then click [Delete].
5. Click [OK]. The readers listing window now list the locks that match the group search criteria.

Settings Form

This form is used to:

- Identify time periods during which to report or to not report ("mask") certain types of information
- Identify time periods during which to activate the reader's outputs
- Select other reader settings such as paired master or slave



Note: Several fields are not available for RS-485 Command Keypad readers.

Listing window

Lists currently defined readers, the access panel to which each is connected, and each reader's type.

Mask Forced Open

Specifies the times during which a forced entry will not be reported as an alarm. Choices in the drop-down list are currently defined timezones. However, when segmentation is enabled, only timezones in the same segment as the selected reader are listed. When alarms are masked, they are not reported to either alarm monitoring or stored in the database for later event reporting.

Mask Held Open

Specifies the times when an alarm will not be reported if the door is held open longer than the **Held Open Time** (from the General form). Choices in the drop-down list are currently defined timezones. However, when segmentation is enabled, only timezones in the same segment as the selected reader are listed. When alarms are masked, they are not reported to either alarm monitoring or stored in the database for later event reporting.

Log Access Grants

Specifies the time period(s) during which the system will log Access Granted events received from this reader. Choices in the drop-down list are currently defined timezones. However, when segmentation is enabled, only timezones in the same segment as the selected reader and timezones assigned to <All Segments> are listed. Access Grants will not be logged during time periods outside of the specified timezone. If no timezone is selected, ALL Access Granted events will be logged to the database.

Log Access Denies

Specifies the time period(s) during which the system will log Access Denied events received from this reader. Choices in the drop-down list are currently defined timezones. However, when segmentation is enabled, only timezones in the same segment as the selected reader and timezones assigned to <All Segments> are listed. Access Denies will not be logged during time periods outside of the specified timezone. If no timezone is selected, ALL Access Denied events will be logged to the database.

Log Reader Status

Specifies the time period(s) during which the system will log Reader Status events received from this reader. Choices in the drop-down list are currently defined timezones. However, when segmentation is enabled, only timezones in the same segment as the selected reader and timezones assigned to <All Segments> are listed. Status events will not be logged during time periods outside of the specified timezone. If no timezone is selected, ALL Status events will be logged to the database.

Paired Master

If selected, indicates that this is a master reader that has an attached slave reader. You must also make sure that the name of the slave reader is selected in the **Slave Reader Attached** field on the Readers form of this folder. A master/slave relationship indicates that the door strike and door contact will be shared between the two readers. This is used when two readers are used to control the same door. An example is when a door is secured for both in and out access. In this case, there will be a reader located on the outside as well as the inside of the door. The master reader controls and reports all door strikes and door contacts, meaning that if a door is forced open, the alarm will be reported for the reader selected as master.

Paired Slave

If selected, indicates that this is a slave reader attached to a master reader. A master/slave relationship indicates that the door strike and door contact will be shared between the two readers. This is used when two readers are used to control the same door. An example is when a door is secured for both in and out access. In this case, there will be a reader located on the outside as well

as the inside of the door. The master reader controls and reports all door strikes and door contacts, meaning that if a door is forced open, the alarm will be reported for the reader selected as master.

Two Card Control

If selected, two cards must always be granted access through the reader in order to open the door.

Deny On Duress PIN

In environments where the reader accepts PIN input, a special duress PIN signals the system that the person attempting entry is in danger (i.e., the person is entering under threat). By default, the door opens in such situations.

If this check box is not selected, access will be granted under duress. The event “Granted Under Duress” or “Granted Under Duress, No Entry” will be generated depending on whether or not the door was opened. Special linkage actions can be associated with these events through the local I/O and global I/O features.

If this check box is selected, access will be denied under duress and the event “Denied Under Duress” will be generated. Special linkage actions can be associated with this event through the local I/O and global I/O features.

Assume Door Used

Selecting this check box will force all valid card swipes to be reported immediately as “Access Granted” events, even if the cardholder did not open the door. If this check box is NOT selected, the event “Access Granted” will not reported until the cardholder opens the door after a valid card swipe. If the door is not used, the event “Access Granted, Door Not Used” will be reported.

Enforce Use Limit

If this check box is selected, badge use limits are enforced at this reader. This means that each time a use-limited badge is used at this reader, the badge’s use limit is decremented for the associated access panel. A cardholder’s use limit is specified on the Badge form of the Cardholders folder.

Whenever the cardholder swipes his badge at a reader where use limits are enforced, the cardholder’s use limit is reduced by one (1). When the use count reaches zero (0), the cardholder is unable to access use limit-enforced card readers on that panel.

A cardholder’s use limit stays in effect until someone manually resets it from within Alarm Monitoring (by right-clicking on the entry for the use limit exceeded alarm) or by manually executing or scheduling a reset use limit action (For more information, refer to Reset Use Limit Properties Window on page 1248.). It should be noted that if a full database download is performed the use limit is preserved.

Some applications of the Use Limit:

- for use by temporary employees or visitors
- for use at readers that control access to commissaries or other locations of supplies, equipment, or provisions. With use limits enforced in these areas, the cardholder’s badge functions like a debit card.

Checkpoint

Select this check box if you want the selected reader to be a designated stop along a guard tour.

First Card Unlock Authority Required

Select this check box if you want special authority to be required for unlocking a door when the reader is in first card unlock mode. If the reader is in “Facility code only” mode, the first card unlock feature does not work.

Turnstile

This check box applies only to readers on Lenel panels that support the Revolving Door Controller turnstile. This check box is not required for other turnstiles.

Select this check box if you have a turnstile model from the Revolving Door Controls company and you want support for multiple access grants while the revolving turnstile is getting previous grants through the turnstile.

When this check box is selected, an access grant pulses the strike output 1 second, regardless of the strike time. This gives the turnstile a count of the number of people it needs to move through the turnstile. If multiple cards are granted entry, the strike output pulses once for each card.

The controller waits the length of the strike time for the door contact input to be activated before issuing a grant with or without entry. Each time the door contact input is activated, the next badge in the queue is issued a grant with entry. The strike time for all other badges in the queue is renewed.

Tailgate

With the tailgate option enabled on the reader, a pulse is sent to the output connected to the tailgate sensor. The tailgate hardware keeps track of how many people enter through a door and generates alarms if a violation is detected.

The output to the tailgate sensor will be auxiliary output 1 and must be configured as such.

A tailgate cannot be configured with an alarm shunt or strike follower because they use auxiliary output 1. Consequently, if **Tailgate** is enabled, **Alarm Shunt** and **Strike Follower** will be deselected.

The tailgate option is for Lenel hardware only.

Alarm Shunt

Supported only with the LNL-2220, LNL-1300, LNL-1320. This option is used to disable generation of an alarm in a secondary intrusion/alarm system when the access control door is used during a valid access grant or REX. When enabled, the auxiliary output 1 relay on the reader interface module will be pulsed in addition to the strike relay and used to intercept the second contact connected to the intrusion/alarm system. The auxiliary output 1 relay will remain energized until just after the door is secured.

An alarm shunt cannot be configured with a tailgate or strike follower because they use auxiliary output 1. Consequently, if **Alarm Shunt** is enabled, **Tailgate** and **Strike Follower** will be deselected.

If you plan to configure an alarm shunt and a pre-alarm, they cannot both use auxiliary output 1. Consequently:

- For the LNL-2220 and LNL-1300 readers, if **Alarm Shunt** is enabled, no pulse aux output option will be available in the **Pre-Alarm mode** drop-down list.
- For the LNL-1320 reader, if **Alarm Shunt** is enabled, select Pre-Alarm mode **Pulse aux output 2**.

Strike Follower

This option is for configuring the output to follow the strike pulse, optionally with a delay or pulse time. When selected, the auxiliary output 1 relay (Output 1 on the Aux Outputs form) is used to define the timing and mode. This feature is supported with the LNL-2220, LNL-3300, Series 2 LNL-1320 or Series 2 LNL-1300.

Strike follower cannot be configured with a tailgate or alarm shunt because they use auxiliary output 1. Consequently, if **Strike Follower** is enabled, **Alarm Shunt** and **Tailgate** will be deselected.

When strike follower is configured, aux output 1 cannot be activated or pulsed in Alarm Monitoring. When strike follower is configured for a reader, output 1 cannot be used for local I/O or global I/O.

If you plan to configure a pre-alarm and strike follower, they cannot both use auxiliary output 1. Consequently:

- For the LNL-2220 and LNL-1300 readers, if **Strike Follower** is enabled, no pulse aux output option will be available in the Pre-Alarm mode drop-down list.
- For the LNL-1320 reader, if **Strike Follower** is enabled, select Pre-Alarm mode **Pulse aux output 2**.

Asset Required

When enabled, an asset is then required to gain access to the reader.

Mask Forced Open

If selected, a forced entry at this door will never be reported as an alarm. If this option is selected, the timezone setting for masking this alarm will have no effect.

Mask Held Open

If selected, indicates that at no time will an alarm be reported if the door is held open longer than the **Held Open Time** (from the General form). If this option is selected, the timezone setting for masking this alarm will have no effect.

Count

Select a number from 0 to 255. A value of 0 indicates that the denied attempts feature will not be used for this reader. When a value greater than 0 is entered, that value indicates the number of times an invalid PIN number can be entered at this reader incorrectly before a “Denied Count Exceeded” transaction is reported. The increment count is based on an invalid PIN for a reader in card and PIN mode, invalid PIN for a reader in PIN or card mode, invalid biometric for a reader in biometric verification mode.

Through local I/O, you can configure a local I/O function list to be executed when the “Deny Count Exceeded” transaction occurs for a given reader. For more information, refer to Chapter 37: Local I/O Folder on page 791.

Through global I/O, you can configure actions to execute when the “Deny Count Exceeded” transaction is reported. For example, you can configure actions that activate an output or lock the reader. For more information please refer to Appendix A: Actions on page 1193.

Timeout

In cases of denied attempts, this field is used to specify the amount of time (in minutes) the controller will use to evaluate the number of denied attempts for a given reader. For example, if the **Timeout** field set to 1, the controller would reset the count of invalid attempts after a period of 1 minute. If the cardholder does not wait for 1 minute, the **Count** field limit is invoked.

Restore

Determine whether a reader will be locked from access requests when the Denied Attempts **Count** value has been reached. Select a number which, in minutes, will determine how long a reader remains locked when the Denied Attempts count has been reached.

For example, assume the **Count** field is set to 5, the **Timeout** field is set to 1, and the **Restore** field is set to 1. If a user enters 5 invalid pin codes at a reader within a 1 minute time period the reader will be automatically locked from processing further access control requests until the 1 minute restore time has elapsed. The mode of the reader cannot be changed once locked until this

time has lapsed. It will also continue to show the original mode the reader was set to prior to the lock out occurring.

A value of 0 indicates the reader will not be locked when the **Denied Attempts Count** has been reached.

Pre-Alarm mode

A pre-alarm alerts cardholders that the door held open time is about to expire and triggers an alarm. To use the pre-alarm, select an option from this drop-down. The options include:

- **None**: No alarm is used.
- **Pulse aux output 1**: On a pre-alarm, a "Door Forced Open" alarm is generated.

Note: If you plan to configure a pre-alarm and an alarm shunt, they cannot both use auxiliary output 1. Consequently: For the LNL-2220 and LNL-1300 readers, if **Alarm Shunt** is enabled, no pulse aux output option will be available in the **Pre-Alarm mode** drop-down list. For the LNL-1320 reader, if **Alarm Shunt** is enabled, select **Pre-Alarm mode** "Pulse aux output 2."

- **Use reader buzzer**: On a pre-alarm the reader buzzer will beep twice every second until the door is closed, ending the pre-alarm.

Note: The Use reader buzzer functionality might not work on every reader. It also requires firmware 3.073 or later.

The pre-alarm is used ONLY in situations where the door is held open after access has been granted. If the door is forced open and a "Door Forced Open" alarm is generated, the pre-alarm is not activated if the held open time expires. You will already be in alarm mode because the door has been forced open, so a pre-alarm is not necessary.

For Lenel hardware, the duration of the reader's auxiliary output 1 is specified on the Aux Outputs tab (**Output 1 Pulse Time** spin button). The default value is five (5) seconds. For Lenel readers, the reader's auxiliary output 1 can be wired to devices such as sounders which can warn the cardholder to close the door before an alarm is triggered.

Pre-Alarm timeout

A pre-alarm alerts cardholders that the door held open time is about to expire and trigger an alarm. Enter when (in seconds) you want the reader's auxiliary output 1 (pre-alarm) activated. The pre-alarm timeout range is 1-131,070 seconds but must be 2 seconds less than the held open time.

LED Mode

This field configures the LED on the reader, and is activated only if the reader is connected to a Lenel access panel. Choices include:

- **1-Wire LED Control** - If selected, LED control will be via a single wire.
- **2-Wire LED Control** - If selected, two wires will be used to control the LED on the reader. This option applies to the LNL-2000 reader and to all other readers that support 2-wire communication.

Note: If you use a 2-wire LED you lose control of the buzzer.

- **Dorado LED Control** - This option is to be used ONLY for readers manufactured by Dorado. Dorado readers are configured differently from the standard 1- or 2-wire LED control.
- **LCD Command Keypad** - Indicates the attached reader is LED/text capable. This LED mode is automatically selected (and cannot be changed) when the reader type is one of the RS-485 Command Keypads.

Modify
Used to configure reader settings.

Help
Displays online assistance for this form.

Multiple Selection
If selected, two or more entries can be simultaneously checked in the listing window.

Close
Closes the Readers folder.

Settings Form Procedures

Use the following procedures on this form.

Configure Reader Settings

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. Click the Settings tab.
3. In the listing window, select the name of the reader to which these settings will apply.
4. Click [Modify].
5. In the During Timezone section, for each action listed select the timezone (if any) during which it is to occur.
6. In the Settings and Always sections, select the check box(es) corresponding to the conditions that you want to occur.
7. In the Denied Attempts section, specify the count and timeout values for this reader.
8. In the Pre-Alarm section, select a Pre-Alarm mode to use a pre-alarm. Enter the number of seconds before the held open time expires that you want pre-alarm to start.

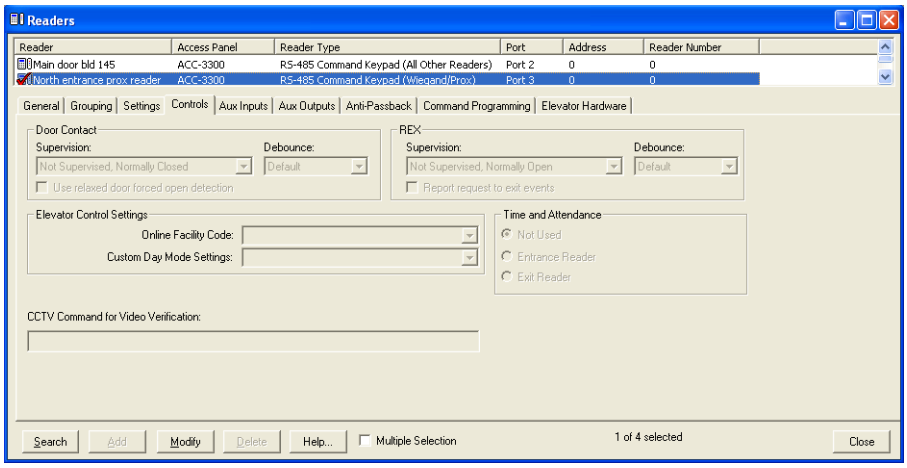
Note: The duration of the pre-alarm is configured on the Aux Outputs tab.

9. If the reader is connected to a Lenel panel, select the appropriate LED mode.
10. Click [OK].

Controls Form

This form is used to:

- Choose elevator access settings, if you are working with an elevator reader.
- Specify the command used in video verification situations, if you are working with an elevator reader and a CCTV camera is installed at this reader.
- Specify global event programming links associated with keypad commands, if you are working with keypad-equipped readers.



Notes: RS-485 Command Keypad readers do not support fields on the Controls form.

For readers connected to HID panels, Door Contact and REX Supervision is supported for System and Basic Custom EOL resistor tables, only. Door Contact and REX Debounce settings are also supported. For more information, refer to Advanced Custom EOL Resistor Tables on page 819.

Door Contact and REX settings are not supported for NGP onboard reader #2.

Listing window

Lists currently defined readers, the access panel to which each is attached, and each reader's type.

Door Contact

Contains the **Supervision** and **Debounce** fields.

Supervision

Lenel hardware only - Select a supervision and normally open/closed setting from the drop-down list. Choices in the drop-down list are based on the EOL tables. There are four built-in tables and up to four custom tables that can be configured by the user. For more information, refer to Chapter 39: EOL Tables Folder on page 819. The four built in tables are:

- Default Supervision, Normally Closed
- Default Supervision, Normally Open
- Not Supervised, Normally Closed
- Not Supervised, Normally Open

Each auxiliary input can be individually wired for either supervised or unsupervised activity. An unsupervised input is an unprotected, low security input. Someone can short-circuit the connection between the auxiliary input and the device controlled by the input, thereby defeating the circuit. Although the device may trigger an alarm condition in such a situation, the auxiliary input will not be aware of it.

By contrast, a supervised input's circuit is equipped with resistors. Subtle changes in the voltage on the circuit can be detected to determine whether someone has tampered with the wiring. For this reason, supervised inputs are high security.

Debounce

Lenel hardware only - Debounce is the amount of time that an input must change state in order for that change to be considered a logical change of state. There are six levels of debounce (1-6). These are relative levels with 1 being the lowest (shortest) and 6 being the highest (longest). It is

up to the hardware interface to map these values to hardware specific values, as well as to map the "Default" option to a hardware specific value. The Lenel hardware interface maps these values to:

- 1 - Lenel value of two scans, ~33 ms (default for REX)
- 2 - Lenel value of four scans, ~67 ms
- 3 - Lenel value of six scans, ~100 ms (default for door contact and alarm and reader aux inputs)
- 4 - Lenel value of nine scans, ~150 ms
- 5 - Lenel value of 12 scans, ~200 ms
- 6 - Lenel value of 15 scans, ~250 ms

Note: It is recommended that the debounce time should not be changed and left at the default setting of "Default."

Use relaxed door forced open detection

Select to allow a small window of time (approximately 3 seconds) after an authorized door entry that the door may be reopened without triggering a door forced open alarm.

REX

Contains the **Supervision** and **Debounce** fields.

Supervision

Lenel hardware only - Select a supervision and normally open/closed setting from the drop-down list. Choices in the drop-down list are based on the EOL tables. There are four built-in tables and up to four custom tables that can be configured by the user. For more information, refer to Chapter 39: EOL Tables Folder on page 819. The four built in tables are:

- Default Supervision, Normally Closed
- Default Supervision, Normally Open
- Not Supervised, Normally Closed
- Not Supervised, Normally Open

Each auxiliary input can be individually wired for either supervised or unsupervised activity. An unsupervised input is an unprotected, low security input. Someone can short-circuit the connection between the auxiliary input and the device controlled by the input, thereby defeating the circuit. Although the device may trigger an alarm condition in such a situation, the auxiliary input will not be aware of it.

By contrast, a supervised input's circuit is equipped with resistors. Subtle changes in the voltage on the circuit can be detected to determine whether someone has tampered with the wiring. For this reason, supervised inputs are high security.

Debounce

Lenel hardware only - Debounce is the amount of time that an input must change state in order for that change to be considered a logical change of state.

There are six levels of debounce (1-6). These are relative levels with 1 being the lowest (shortest) and 6 being the highest (longest). It is up to the hardware interface to map these values to hardware specific values, as well as to map the "Default" option to a hardware specific value. The Lenel hardware interface maps these values to:

- 1 - Lenel value of two scans, ~33 ms (default for REX)
- 2 - Lenel value of four scans, ~67 ms
- 3 - Lenel value of six scans, ~100 ms (default for door contact and alarm and reader aux inputs)

- 4 - Lenel value of nine scans, ~150 ms
- 5 - Lenel value of 12 scans, ~200 ms
- 6 - Lenel value of 15 scans, ~250 ms

Note: It is recommended that the debounce time should not be changed and left at the default setting of "Default."

Report request to exit events

Click to enable. By enabling the check box the request to exit events are reported to Alarm Monitoring and logged in the database.

Elevator Control Settings

This section is activated only when an elevator reader is selected. A reader is configured as an elevator reader if the **Elevator** check box is selected on the General form of the Readers folder. This section includes the **Standard Day Mode Timezone**, **Custom Day Mode Settings**, **Standard Day Mode/Facility Code Settings** OR **Online Facility Code** and **Custom Day Mode Settings** fields.

Online Facility Code

When the Reader and Alarm Output Panel(s) are online:

- Online facility code grants will gain access to any floor listed in the **Online Facility Code** drop-down list, if the current time is within the timezone for that floor. Each floor listed in the drop-down list can have its own timezone, which is configured on the Elevator Control form of the Access Levels folder.
- Access to floors occurs regardless of the **Enable Floor When Using Facility Code** check box setting on the Elevator Control form in the Access Levels folder.
- The Online Facility Code feature applies to 6 floor Lenel elevator control with Dual Reader interface and extended Lenel elevator control with Single Reader interface modules configured to support facility code operation.

When the Reader and/or Alarm Output Panel(s) are offline:

- Offline facility code floor access is not supported by Lenel elevator readers. For extended elevator control using a Single Reader Interface and alarm panels, no floor access can be gained through an offline facility code grant.
- For 6 floor dual reader elevator control, the first floor output is always activated upon an offline facility code grant.
- For 6 floor dual reader elevator control, if the reader goes offline and offline mode is facility code only, the first output will be activated upon a facility code grant. If the offline mode is unlocked, the first floor will be active while the reader is offline. To prevent this, the offline mode must be locked.

Custom Day Mode Settings

Selects the elevator control level that will be used for access to floors via this reader. Elevator control levels are defined on the Elevator Control form of the Access Levels folder.

- Cardholder grants will gain access to any floor listed in the **Online Facility Code** drop-down list, if the current time is within the timezone for that floor. Each floor listed in the drop-down list can have its own timezone, which is configured on the Elevator Control form of the Access Levels folder.
- Access to floors occurs regardless of the **Enable Floor During Day Mode** check box setting on the Elevator Control form in the Access Levels folder.

– When using floor tracking for extended elevator control with a Dual Reader Interface, the outputs do not light up until the button is pressed.

CCTV Command for Video Verification

Indicates the CCTV command to be used to display live video during video verification. The command specified in this box will be sent to the CCTV switcher for all card events specified for this reader during video verification. This reader must be monitored in the video verification window in order for the command to be sent.

The command must be a command string that your organization's CCTV equipment understands. If your equipment uses control characters as commands, refer to the special note following the procedures in the Alarm Configuration folder chapter, CCTV Instructions form.

Time and Attendance

Includes the **Not Used**, **Entrance Reader**, and **Exit Reader** fields. These fields are used for reporting purposes only, for installations that have time and attendance systems. These fields have no effect on the behavior of the readers.

Not Used

If selected, this reader will not be used for time and attendance reporting.

Entrance Reader

If selected, this reader will be identified as an entrance reader for time and attendance reporting.

Exit Reader

If selected, this reader will be identified as an exit reader for time and attendance reporting.

Modify

Used to configure reader controls.

Help

Displays online assistance for this form.

Multiple Selection

If selected, two or more entries can be simultaneously checked in the listing window.

Close

Closes the Readers folder.

Controls Form Procedures

Use the following procedures on this form.

Configure Reader Controls

Note: Dimmed fields indicate that the corresponding capabilities are not available for the selected reader.

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. Select the Controls tab.

3. In the listing window, select the reader for which to configure reader controls. If the **Multiple Selection** check box is selected, you can select more than one reader at the same time, but will not be able to configure all fields on the form in multiple selection mode.
4. Click [Modify].
5. For Lenel hardware only, in the Door Contact and REX sections:
   a. Select supervision and normally open/closed settings from the **Supervision** drop-down lists.
   b. It is recommended that the debounce time should not be changed and left at the default setting of "Default." However, if you want to change this value, select an option from the **Debounce** drop-down list. Debounce is the amount of time that an input must change state in order for that change to be considered a logical change of state. There are six levels of debounce (1-6). These are relative levels with 1 being the lowest (shortest) and 6 being the highest (longest). It is up to the hardware interface to map these values to hardware specific values, as well as to map the "Default" option to a hardware specific value. The Lenel hardware interface maps these values to:
      - 1 - Lenel value of two scans, ~33 ms (default for REX)
      - 2 - Lenel value of four scans, ~67 ms
      - 3 - Lenel value of six scans, ~100 ms (default for door contact and alarm and reader aux inputs)
      - 4 - Lenel value of nine scans, ~150 ms
      - 5 - Lenel value of 12 scans, ~200 ms
      - 6 - Lenel value of 15 scans, ~250 ms

Note: The **Debounce** field is available for Lenel hardware only.

6. If the reader is an elevator reader, choose elevator control settings.
7. If your system is integrated with a time and attendance system, indicate whether you wish to identify the reader (for reporting or data exporting purposes) as an entrance reader, exit reader, or neither.
8. If a CCTV camera is installed at this reader, specify the command for video verification.
9. If the reader is a keypad reader, enter the cipher code (up to six digits) that can be used to unlock the reader when it is in cipher mode.
10. Click [OK].

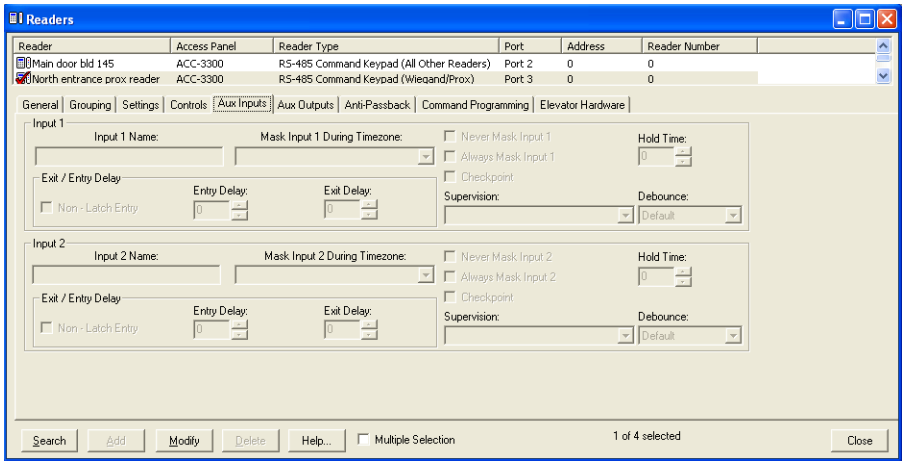
Aux Inputs Form

Each reader has one or more auxiliary inputs that can be connected to and can monitor a set of dry (non-powered) contacts. When a closure of the contacts is detected the reader generates an auxiliary alarm.

If the reader is a Lenel elevator reader (i.e., if it is reader #1 on an LNL-1320 Dual Reader Interface board, and the **Elevator** check box is selected on the General form of this folder), then inputs 1 and 2 are used as the auxiliary inputs. The other six inputs are reserved for future use.

Functions:

- Assign a name to each of a reader's auxiliary inputs
- Specify the times during which auxiliary input alarms will not be reported to the system



Notes: RS-485 Command Keypad readers do not support auxiliary inputs.

LNL-2210 on-board readers do not support auxiliary inputs.

Listing window

Lists currently defined readers, the access panel to which each is attached, and each reader's type.

Input # Name

Enter a unique, descriptive name for this reader's auxiliary input # 1 or 2. If this field is configured, alarms generated from the aux 1 or 2 input will be displayed in alarm monitoring with the name entered in this field.

Mask Input # During Timezone

Lenel hardware only - Select the timezone (if any) during which to not report alarms from this reader's auxiliary input #1or 2. Choices include all currently defined timezones.

Never Mask Input

If selected, alarms originating at this reader's auxiliary input #1 or 2 will always be reported. For those inputs marked as such the mask and unmask options in the software will be disabled.

Always Mask Input

If selected, alarms originating at this reader's auxiliary input #1 or 2 will never be reported.

Checkpoint

Select this check box if the reader's auxiliary input #1 or 2 is wired as a checkpoint (a designated stop along a guard tour).

Hold Time

When an input goes active and is restored, enter the amount of time (in seconds) to wait until reporting the input as restored. If the input goes active again within the hold time, a change of state is not reported, but just remains as active. You can enter a value of 0 to 15 seconds.

This feature is useful when there is no advantage to log the specific number of times a point is tripped after the initial event. For example, if a motion detector is tripped into active, the state remains there for the hold time after the last motion event is detected.

Supervision

Select a supervision and normally open/closed setting from the drop-down list. Choices in the drop-down list are based on the EOL tables. There are four built-in tables and up to four custom tables that can be configured by the user. For more information, refer to Chapter 39: EOL Tables Folder on page 819. The four built-sin tables are:

- Default Supervision, Normally Closed
- Default Supervision, Normally Open
- Not Supervised, Normally Closed
- Not Supervised, Normally Open

You can configure up to eight (8) different EOL tables per panel.

Each auxiliary input can be individually wired for either supervised or unsupervised activity. An unsupervised input is an unprotected, low security input. Someone can short-circuit the connection between the auxiliary input and the device controlled by the input, thereby defeating the circuit. Although the device may trigger an alarm condition in such a situation, the auxiliary input will not be aware of it.

By contrast, a supervised input's circuit is equipped with resistors. Subtle changes in the voltage on the circuit can be detected to determine whether someone has tampered with the wiring. For this reason, supervised inputs are high security.

Debounce

Lenel hardware only - *Debounce* is the amount of time that an input must change state in order for that change to be considered a logical change of state. There are six levels of debounce (1-6). These are relative levels with 1 being the lowest (shortest) and 6 being the highest (longest). It is up to the hardware interface to map these values to hardware specific values, as well as to map the "Default" option to a hardware specific value. The Lenel hardware interface maps these values to:

- 1 - Lenel value of two scans, ~33 ms (default for REX)
- 2 - Lenel value of four scans, ~67 ms
- 3 - Lenel value of six scans, ~100 ms (default for door contact and alarm and reader aux inputs)
- 4 - Lenel value of nine scans, ~150 ms
- 5 - Lenel value of 12 scans, ~200 ms
- 6 - Lenel value of 15 scans, ~250 ms

Note: It is recommended that the debounce time should not be changed and left at the default setting of "Default."

Non-Latch Entry

Lenel hardware only - Non-latch entry is used in conjunction with the **Entry Delay** field. When checked, the **Entry Delay** being configured will be a Non-Latch entry delay.

Entry Delay

Lenel hardware only - Entry delay is used in conjunction with the **Non-Latch Entry** field.

If the **Non-Latch Entry** check box is selected (i.e. non-latched mode), when auxiliary input 2 is active the alarm will NOT be reported until the **Entry Delay** time expires. The alarm will only be reported if the input is still active at the end of the specified delay. Application: false alarm prevention such as invalid motion detector reads.

If the **Non-Latch Entry** check box is not selected (i.e. latched mode), when auxiliary input 2 is active the alarm WILL be reported unless the input is masked (either automatically through the

software or manually via a keypad) within the specified delay after the alarm input goes active. Application: valid access to a room with motion detectors.

Exit Delay

Lenel hardware only - Specifies the delay (in seconds) for auxiliary input 2 to switch from a masked state to an unmasked state. You can choose a value in the range of 0 through 32767.

When an auxiliary input is unmasked, active alarms will NOT be reported until the **Exit Delay** expires. Application: securing a room upon exit (such as activating motion detectors).

Modify

Changes the auxiliary output configuration for the selected reader.

Help

Displays online assistance for this form.

Multiple Selection

If selected, two or more entries can be simultaneously checked in the listing window.

Close

Closes the Readers folder.

Aux Inputs Form Procedures

Use the following procedures on this form.

Configure Reader Input(s)

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. Click the Aux Inputs tab.
3. In the listing window, select the reader for which to configure the auxiliary input(s).
4. Click [Modify].
5. From the reader's type (as defined on the Readers form) the application automatically determines the number of auxiliary inputs. Dimmed fields indicate that the corresponding inputs are not configurable for the selected type of reader.
6. For each input, type a name and indicate when to mask the input.
7. If the reader is a Lenel reader, you can choose non-latched mode and configure entry and exit delays.
8. Click [OK].

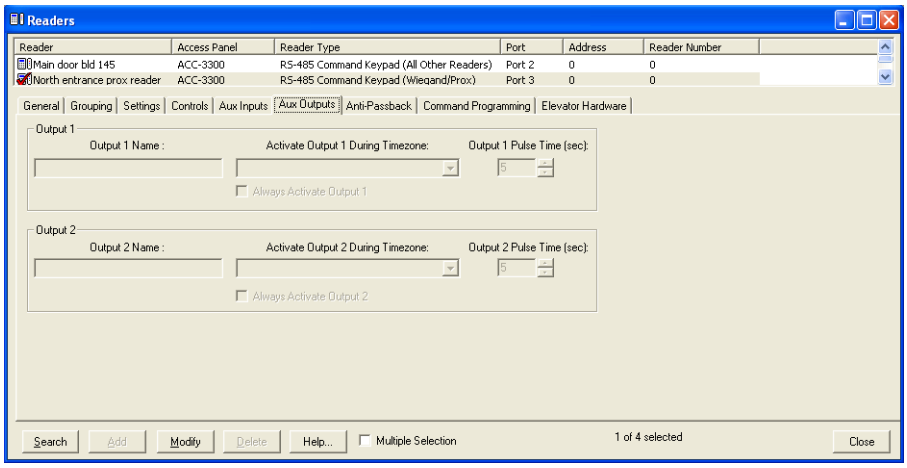
Aux Outputs Form

This form is used to:

- Assign a name to each of a reader's auxiliary outputs
- Specify the pulse time for each output
- Configure strike follower timing (when enabled on the Settings form)

Note that auxiliary outputs are not supported for a Lenel elevator reader (reader #1 on an LNL-1320 Dual Reader Interface board, and the **Elevator** check box is selected on the General form of this folder).

If LNL-2210 on-board reader #1 is selected, only Output 1 is supported. Auxiliary outputs are not supported if a second LNL-2210 on-board reader is selected.



Note: RS-485 Command Keypad readers do not support auxiliary outputs.

Listing window

Lists currently defined readers, the access panel to which each is attached, and each reader's type.

Output 1 Name

Use this field to specify a unique, descriptive name for this reader's output #1.

Activate Output 1 During Timezone

Specifies the time period(s) when auxiliary output #1 is to be active. Available choices are the currently defined timezones.

Output 1 Pulse Time (sec)

You can pulse (turn on then off again) reader output #1 from within the software. Use this field to specify the duration of the pulse, in seconds.

Always Activate Output 1

This field specifies that the output will be always in an active ("on") state. If you select this check box, you cannot choose a timezone in the **Activate Output 1 During Timezone** field (because the output will be active during all timezones).

Strike Follower Mode

This field appears when **Strike Follower** is configured on the Settings form.

When strike follower is enabled (through an option on the Settings form) output 1 is used for strike follower configuration. (The strike time and cut off are defined on the General form.) (See Configure Strike Follower, on page 662 for details.)

Delay time

This field appears when **Strike Follower** is configured on the Settings form.

Use this field to enter the duration of delay between activation of the strike and activation of the aux 1 output (in seconds). The delay can be set from 0 (no delay) to 6 seconds.

Pulse time

This field appears when **Strike Follower** is configured on the Settings form and when Strike Follower Mode is set to **Pulse**.

From the drop-down, select the duration of the pulse (in seconds) for the output. The pulse time can be set from 0.5 to 2.0 seconds.

Output 2 Name

Use this field to specify a unique, descriptive name for this reader's output #2.

Activate Output 2 During Timezone

Specifies the time period(s) when auxiliary output #2 is to be active. Available choices are the currently defined timezones.

Output 2 Pulse Time (sec)

You can pulse (turn on then off again) reader output #2 from within the software. Use this field to specify the duration of the pulse, in seconds.

Always Activate Output 2

This field specifies that the output will be always in an active ("on") state. If you select this check box, you cannot choose a timezone in the **Activate Output 2 During Timezone** field (because the output will be active during all timezones).

Modify

Changes the auxiliary output configuration for the selected reader.

Help

Displays online assistance for this form.

Multiple Selection

If selected, two or more entries can be simultaneously checked in the listing window.

Close

Closes the Readers folder.

Aux Outputs Form Procedures

Use the following procedures on this form.

Configure Reader Output(s)

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. Click the Aux Outputs tab.
3. In the listing window, select the reader for which to configure the auxiliary output(s).

   If the **Multiple Selection** check box is selected, you can select more than one reader at the same time, but you can't name outputs while in multiple selection mode.
4. Click [Modify].
5. From the reader's type (as defined on the Readers form) the application automatically determines the number of auxiliary outputs. Dimmed fields indicate that the corresponding outputs are not configurable for the selected type of reader.

6. For each output, type a name and indicate when to activate the output.
7. Indicate the pulse time in seconds.
8. Click [OK].

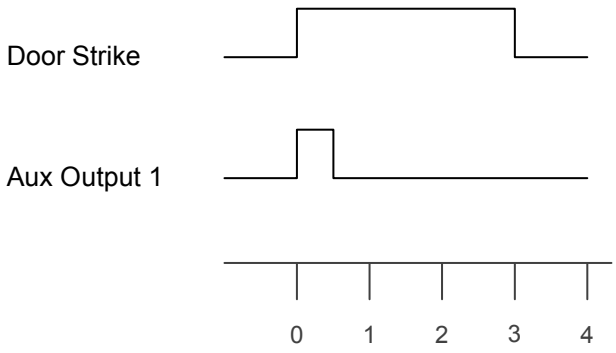
Configure Strike Follower

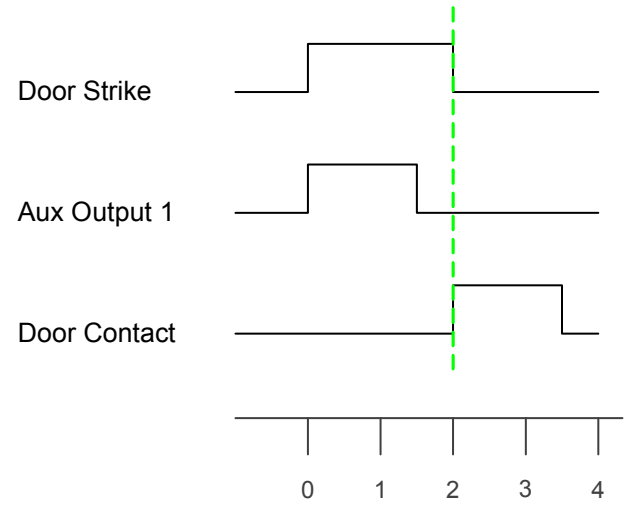
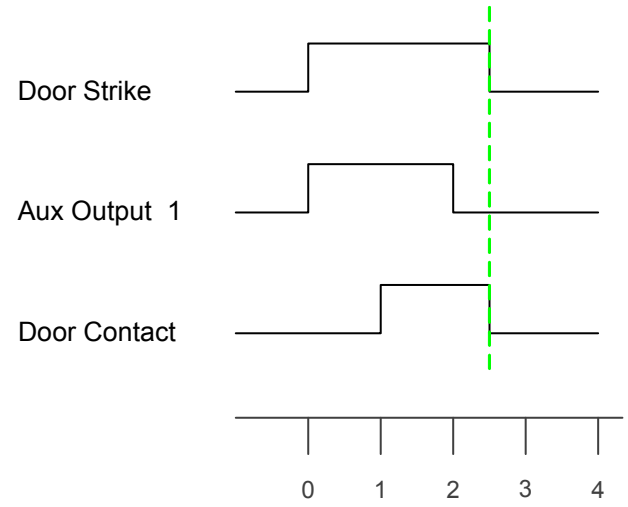
1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. On the General form, choose a reader. Enter the **Strike Time** and choose the **Strike** cut off for the reader.
3. On the Settings form, select the **Strike Follower** check box.
4. Since Strike Follower was selected, on the Aux Outputs form, Output 1 becomes the Strike Follower. If the reader type selected does not have any outputs, then strike follower cannot be configured.
5. For the **Delay**, enter the duration of delay between the strike and aux output 1 (in seconds). The delay can be set from 0 (no delay) to 6 seconds.
6. For the Strike Follower Mode, select **Follower** or **Pulse**.
7. If pulse mode was selected, from the drop-down, select the duration of the **Pulse Time** (in seconds) for the output. The Pulse time can be set from 0.5 to 2.0 seconds.
8. Click [OK].

The following tables show a visual depiction of the timing of the door strike and follower, with sample data chosen for the delay and pulse times.

Pulse Mode

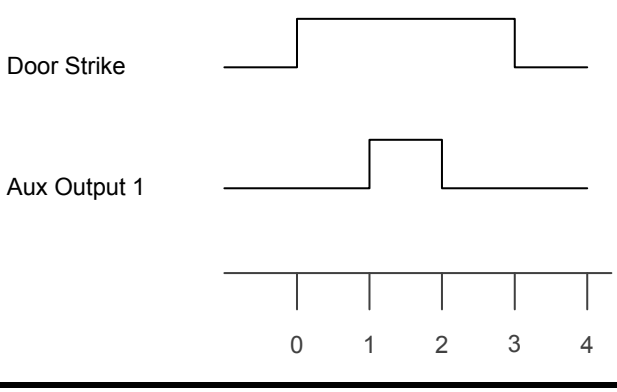
In this configuration, the strike and aux output 1 are activated at the same time, with aux output 1 remaining energized for the specified pulse time.

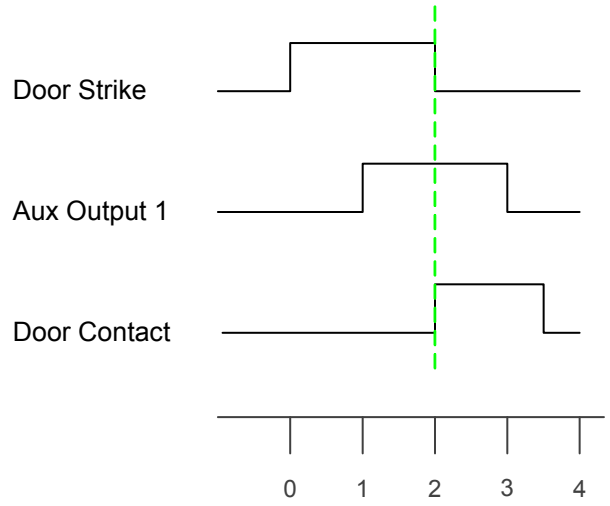
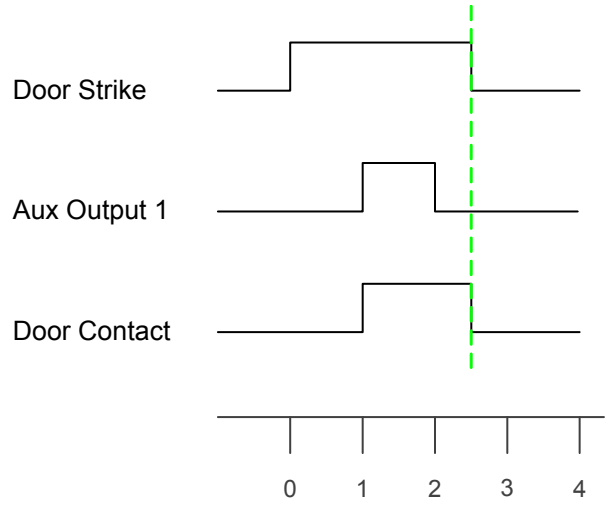
Delay = 0 Pulse mode Pulse = 0.5 The door is not opened.	

Delay = 0 Pulse mode Pulse = 1.5 The door is opened and the strike is set to cut off on open.	
Delay = 0 Pulse mode Pulse = 2 The door is opened and the strike is set to cut off on close.	

Delayed Pulse Mode

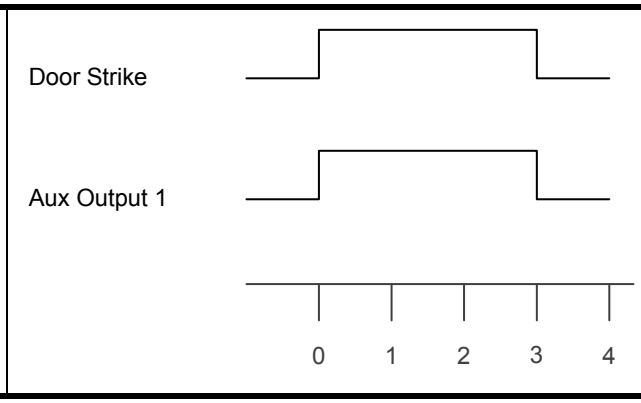
In this configuration, the strike activates first. After the specified delay time, the aux output 1 activates. After the specified pulse time, aux output 1 should deactivate. Note that aux output 1 will only activate if the delay time is within the time of the strike being energized.

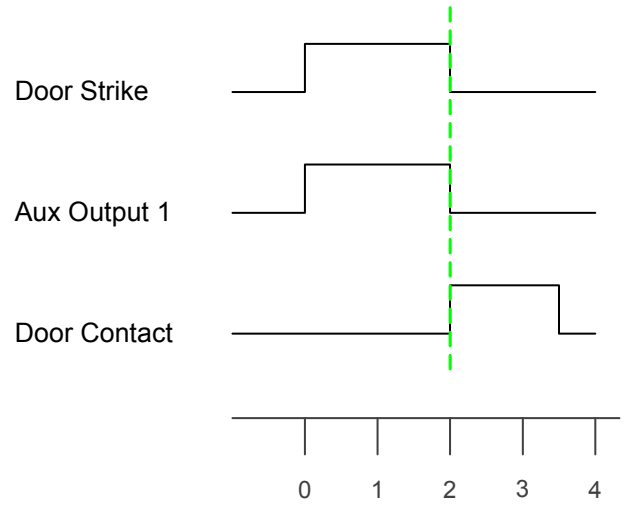
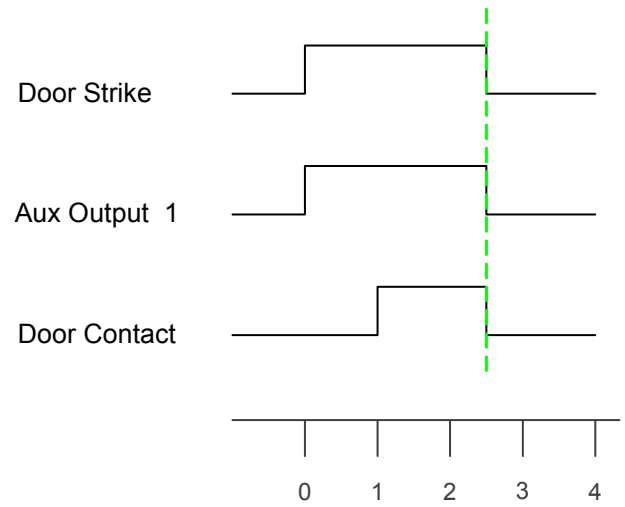
Delay = 1 Pulse mode Pulse = 1 The door is not opened.	

Delay = 1 Pulse mode Pulse = 2 The door is opened and the strike is set to cut off on open.	
Delay = 1 Pulse mode Pulse = 1 The door is opened and the strike is set to cut off on close.	

Follower Mode

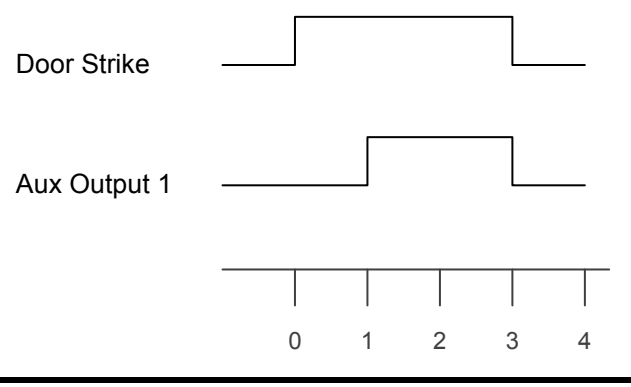
In this configuration, the strike and aux output 1 activate and deactivate at the same time.

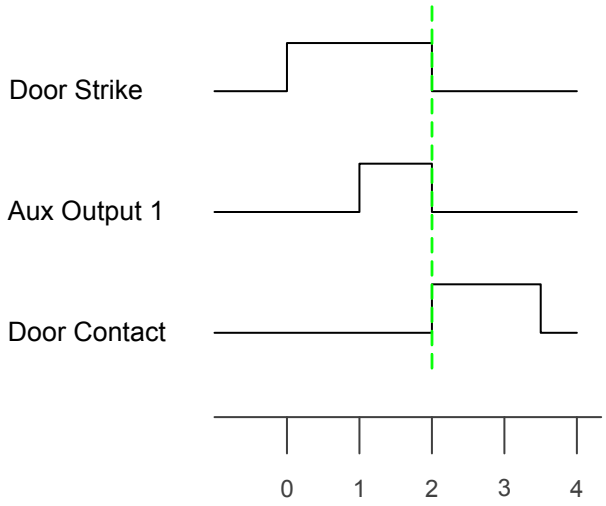
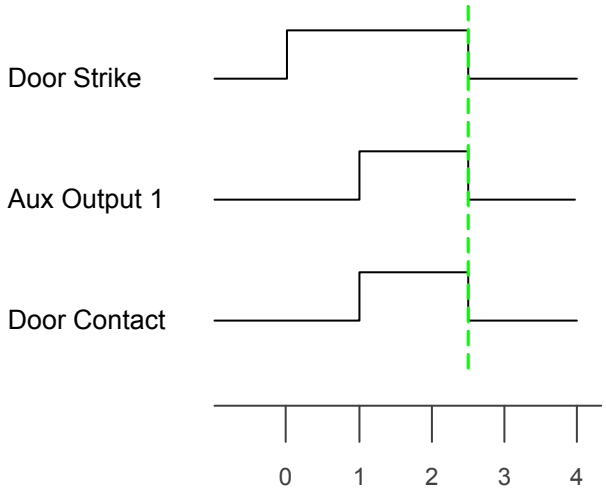
Delay = 0 Follower mode Pulse not applicable The door is not opened.	

Delay = 0 Follower mode Pulse not applicable The door is opened and the strike is set to cut off on open.	
Delay = 0 Follower mode Pulse not applicable The door is opened and the strike is set to cut off on close.	

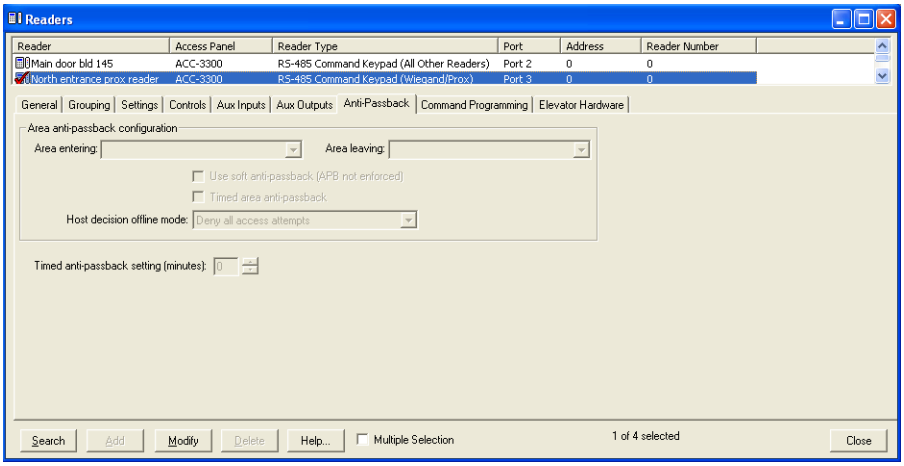
Delayed Follower Mode

In this configuration, the strike activates, and then aux output 1 activates after the specified delay time. When the strike deactivates, aux output 1 also deactivates. Note that aux output 1 will only activate if the delay time is within the time of the strike being energized.

Delay = 1 Follower mode Pulse not applicable The door is not opened.	

Delay = 1 Follower mode Pulse not applicable The door is opened and the strike is set to cut off on open.	
Delay = 1 Follower mode Pulse not applicable The door is opened and the strike is set to cut off on close.	

Anti-Passback Form



Listing window

Lists currently defined readers, the access panel to which each is attached, and each reader's type.

Area entering

Selects the area a cardholder enters by using this reader. Named areas are defined on the Anti-Passback Areas form of the Areas folder. Area anti-passback prevents a cardholder from gaining access to an area without first using his/her card to move out of the area.

Area leaving

Selects the area a cardholder exits by using this reader. Choices include:

- Named areas - Areas that are defined on the Anti-Passback Areas form of the Areas folder.
- <Don't Care> - Setting used by Global Anti-Passback and Local Anti-Passback to indicate that the anti-passback rules do not care about the area leaving.

Note: With a Lenel controller, if you attempt to enter an area you are already in an APB violation will be noted.

Use soft anti-passback (APB not enforced)

Select this check box to enable soft anti-passback at this reader. This means that access will be granted even if an anti-passback violation occurs. In this case, the user is still permitted access to the reader and an anti-passback violation is reported to Alarm Monitoring.

Timed area anti-passback

Select this check box to enable timed area anti-passback for the selected reader. Timed area anti-passback provides the behavior of timed anti-passback but across a group of readers in the same area. For example, in office buildings with multiple readers that access the same area.

Timed area anti-passback allows you to configure how many minutes (configurable by the **Timed anti-passback settings (minutes)** scroll button) a person must wait before they are able to use their card again at the specified readers. If the reader is used before the time allotted has passed the cardholder will be denied access and an "Anti-Passback Violation" will be reported in Alarm Monitoring. If the reader is used after the time allotted has passed the cardholder is still granted access but a "Granted, APB Violation" is reported in Alarm Monitoring.

For Timed area anti-passback to work you must enable both the **Store area anti-passback location** and **Timed anti-passback** check boxes on the Options tab in the Access Panels form.

You must NOT configure global anti-passback for the system or segment a reader belongs to if that reader has already been configured for timed area anti-passback. If you do the timed area anti-passback will be turned off.

Host decision offline mode

This option is used for Global Anti-Passback to inform the panel what to do in case the panel is offline from the host. For this option to be available, you must:

- Have Global Anti-Passback enabled. On non-segmented systems, this is done by selecting the **Global Anti-Passback** check box on the Anti-Passback form in the System Options folder. On segmented systems, this check box is available on the Anti-Passback sub-tab of the Segments form in the Segments folder.
- Select an **Area entering** on this form.
- Deselect the **Use soft-anti-passback (APB not enforced)** check box on this form.

For Global Anti-Passback, the panel requests a decision from the host to determine if the cardholder will be allowed access to the reader. When the panel is offline from the host this request cannot be performed, so the panel will allow access based on this setting. Choices include:

- Deny all access attempts - All access attempts at this reader when the panel is offline with the host will be denied.
- Make local decision at panel - All access attempts at this reader when the panel is offline will be granted access based on the local settings in the panel (proper access level, etc.).

Timed anti-passback setting (minutes)

Specifies the length of time (in minutes) after this reader is used before it can be used again. Timed anti-passback differs functionally from area anti-passback. When timed anti-passback is used at a reader, the cardholder cannot use their card at the reader with timed anti-passback enabled until AFTER the anti-passback time has expired OR their card is used to gain valid access to another reader.

For this option to be available, you cannot have an **Area entering or Area leaving** selected, and the **Use soft anti-passback (APB not enforced)** check box cannot be selected.

This setting also applies to the area anti-passback configuration if the **Timed area anti-passback** options has been selected.

Modify

Click this button to change the area anti-passback configuration for the selected reader.

Help

Displays online assistance for this form.

Multiple Selection

If selected, two or more entries can be simultaneously checked in the listing window.

Close

Closes the Readers folder.

Anti-Passback Form Procedures

Use the following procedures for this form.

Configure Area Anti-Passback

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. Click the Anti-Passback tab.
3. In the listing window, select the reader for which to configure area anti-passback. If the **Multiple Selection** check box is selected, you can select more than one reader at the same time.
4. Click [Modify].
5. In the **Area entering** field, select the area a cardholder enters when he/she uses this reader.
6. In the **Area leaving** field, select the area a cardholder exits when he/she uses this reader.
7. Select one of the following:
   a. **Use soft anti-passback (APB not enforced)** - Select if you want to enable soft anti-passback at this reader. When selected, access will be granted even if an anti-passback violation occurs. In this case, the user is still permitted access to the reader and an anti-passback violation is reported to Alarm Monitoring.
   b. **Timed area anti-passback** - Select if you want to enable timed area anti-passback at this reader.

Note: If you select the **Use soft anti-passback (APB not enforced)** check box, the **Host decision offline mode** drop-down list will be disabled.

8. If you've selected the **Use soft anti-passback (APB not enforced)** or **Timed area anti-passback** check box, skip this step. Otherwise, select the **Host decision offline mode**.

   This option is used for Global Anti-Passback to inform the panel what to do in case the panel is offline from the host. Choices include:

   - Deny all access attempts - All access attempts at this reader when the panel is offline with the host will be denied.
   - Make local decision at panel - All access attempts at this reader when the panel is offline will be granted access based on the local settings in the panel (proper access level, etc.).

Note: For this field to be available for selection, you must have Global Anti-Passback enabled. On non-segmented systems, this is done by selecting the **Global Anti-Passback** check box on the Anti-Passback form in the System Options folder. On segmented systems, this check box is available on the Anti-Passback sub-tab of the Segments form in the Segments folder.

9. Click [OK].

Configure Timed Anti-Passback

Note: These steps are also used when you select the **Timed area anti-passback** check box on the Anti-passback form.

Timed anti-passback differs functionally from area anti-passback. When timed anti-passback is used at a reader, the cardholder cannot use their card at the reader with timed anti-passback enabled until AFTER the anti-passback time has expired OR their card is used to gain valid access to another reader. To configure timed anti-passback:

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. Click the Anti-Passback tab.
3. In the listing window, select the reader for which to configure timed anti-passback. If the **Multiple Selection** check box is selected, you can select more than one reader at the same time.
4. Click [Modify].
5. In the **Timed Anti-passback setting (minutes)** field, specify the length of time (in minutes) after this reader is used before it can be used again.

Note: For this option to be available, you cannot have an **Area entering** or **Area leaving** selected, and the **Use soft anti-passback (APB not enforced)** check box cannot be selected.

6. Click [OK].
7. Click [OK] to confirm the modification.

Command Programming Form

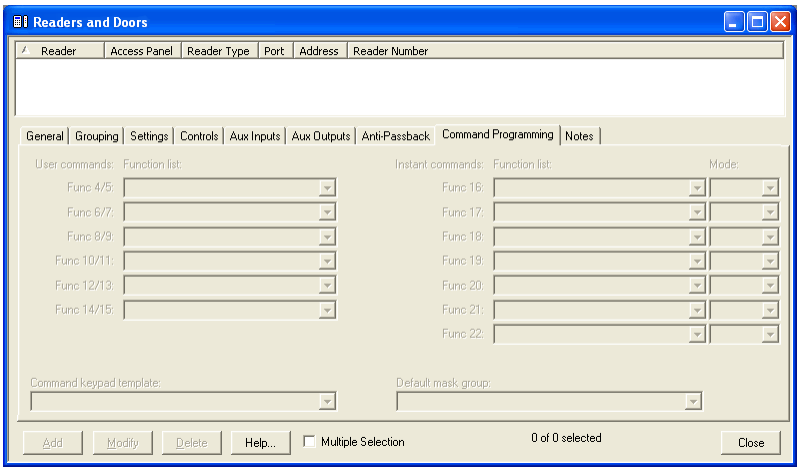
Keypad-equipped readers can have one or more keypad-activated commands programmed into the access panel. These commands (function lists) can be accessed by assigning the function lists to certain keypad sequences. Users of the keypad can invoke these function lists only if they are given permission to execute function lists. This is determined during access level configuration in the

Access Levels folder. All commands are paired functionally; one activates a condition and the second deactivates the condition.

This form is used to link the built-in keypad commands to lists of actions defined elsewhere in the software. This feature is part of the software's global event programming capability.

The fields on this form are arranged in pairs. The left column lists keypad commands available from the selected reader. For each, you specify both a local I/O function list and a logic term of that list. In order to make these selections there must be at least one Local I/O function list defined for the associated access panel. This section is activated only under the following conditions:

- For the selected reader, the **Allow User Commands** check box is selected on the General form of the Readers folder.
- The user wishing to enter keypad commands has an access level that was defined with the **Command Authority for Users** check box selected. This is done on the Access Levels form of the Access Levels folder.



Note: Several fields are not available for RS-485 Command Keypad readers.

Listing window

Lists currently defined readers, the access panel to which each is attached, and each reader's type.

Func 4/5

Select the local I/O function list to link to the Func 4/5 keypad command. Choices include all currently defined Local I/O function lists, which are defined on the Local I/O Function Lists form of the Local I/O folder. The Func 4/5 pair of commands is available on all keypad readers connected to an LNL-1000. If the selected reader is not intelligent, this field is not available.

Func 6/7

Select the local I/O function list to link to the Func 6/7 keypad command. Choices include all currently defined Local I/O function lists, which are defined on the Local I/O Function Lists form of the Local I/O folder. The Func 6/7 pair of commands is available on all keypad readers connected to an LNL-1000. If the selected reader is not intelligent, this field is not available.

Func 8/9

Select the local I/O function list to link to the Func 8/9 keypad command. Choices include all currently defined Local I/O function lists, which are defined on the Local I/O Function Lists form of the Local I/O folder. The Func 8/9 pair of commands is available for all keypad readers connected to an LNL-1000. If the selected reader is not intelligent, this field is not available.

Func 10/11

Select the local I/O function list to link to the Func 10/11 keypad command. Choices include all currently defined Local I/O function lists, which are defined on the Local I/O Function Lists form of the Local I/O folder. The Func 10/11 pair of commands is available for all keypad readers connected to an LNL-1000. If the selected reader is not intelligent, this field is not available.

Func 12/13

Select the local I/O function list to link to the Func 12/13 keypad command. Choices include all currently defined Local I/O function lists, which are defined on the Local I/O Function Lists form of the Local I/O folder. The Func 12/13 pair of commands is available for all keypad readers connected to an LNL-1000. If the selected reader is not intelligent, this field is not available.

Func 14/15

Select the local I/O function list to link to the Func 14/15 keypad command. Choices include all currently defined Local I/O function lists, which are defined on the Local I/O Function Lists form of the Local I/O folder. The Func 14/15 pair of commands is available for all keypad readers connected to an LNL-1000. If the selected reader is not intelligent, this field is not available.

Func 16-22

These functions are non-paired commands used to execute local I/O function lists. These commands can be executed at the reader by inputting “*16#” - “*22#”. These commands do not require command authority in order to be executed.

Mode

Used in conjunction with func 16 through func 22. The **Mode** field determines the action of the function and can be set to “True,” “False,” and “Pulse.”

Command keypad template

Select the command keypad template you would like associated with this reader. For more information, refer to Command Keypad Templates Folder on page 743.

Default alarm mask group

Select the alarm mask group that is to be the default mask group for readers. For more information, refer to Command Keypad Templates Folder on page 743.

Modify

Used to program reader keypad commands.

Help

Displays online assistance for this form.

Multiple Selection

If selected, two or more entries can be simultaneously checked in the listing window.

Close

Closes the Readers folder.

Command Programming Form Procedures

Use the following procedures on this form.

Program Reader Keypad Commands

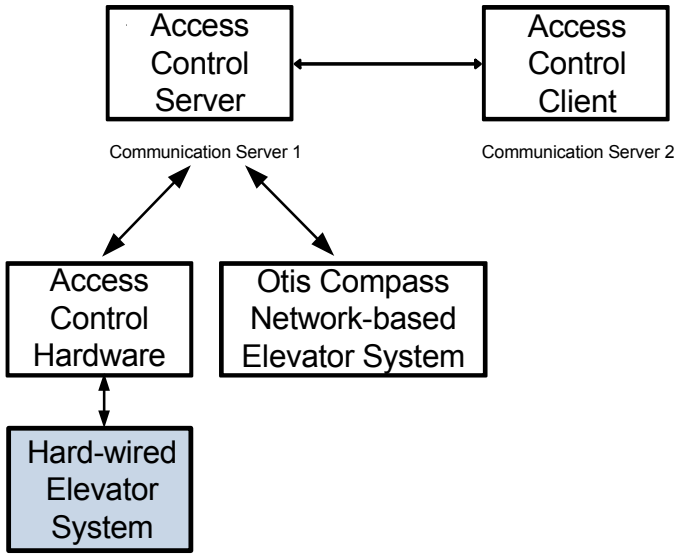
Dimmed fields indicate that the corresponding capabilities are not available for the selected reader.

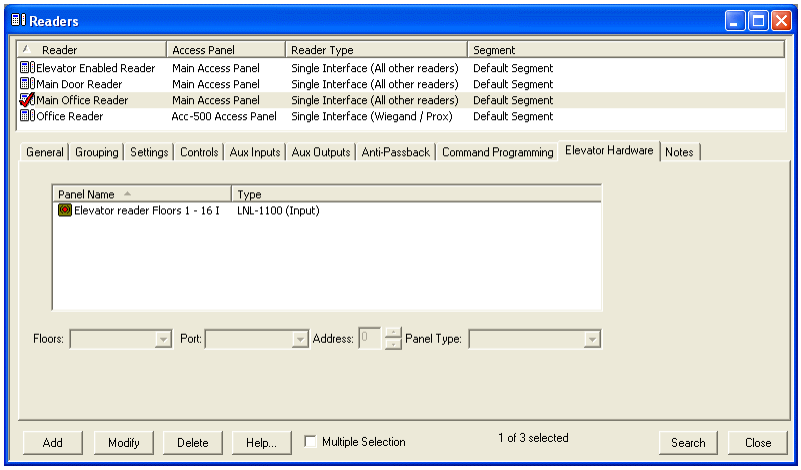
1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. Click the Command Programming tab.
3. In the listing window, select the reader for which to program the keypad commands. If the **Multiple Selection** check box is selected, you can select more than one reader at the same time.
4. Click [Modify].
5. If the reader has a keypad, create links between keypad commands and local I/O function lists. For each pair of commands, select a **Function List** to trigger. At least one function list must have been defined for the associated access panel.
6. Click [OK].

Elevator Hardware Form

Notes: This section describes the configuration of a hard-wired elevator system. Various solutions can be configured using Lenel hardware including the LNL-1300 panel (6 floors; no floor tracking) or LNL-1320 panel (128 floors; floor tracking optional). NGP access panels do not support elevator configuration.

For Otis Compass elevator systems: Use the Elevator Dispatching Devices and Elevator Terminal forms. For more information, refer to Elevator Dispatching Configuration Overview on page 836.





Note: RS-485 Command Keypad readers do not support elevator control.

Listing window

Lists currently defined readers, the access panel to which each is attached, and each reader's type.

Assignment window

Lists currently defined alarm panels used for elevator control with the selected reader. You can sort the list by the alarm panel names or by their type.

Floors

Indicates the range of outputs or inputs that this panel controls. Each input or output can be wired to control access to one or multiple floors, gates, etc.

Port

Indicates the access panel port that this alarm panel is connected to. Each access panel has communication ports used for field hardware devices such as readers or alarm panels. An LNL-1000 access panel can have 2 to 4 ports (ports # 2-5), depending on configuration. An LNL-500 has ports 2 and 3. Two-wire and/or four-wire communication can be used, depending upon configuration.

There can be up to 32 devices (but no more than 16 alarm panels) connected to each port on an LNL-1000 access panel. There can be up to 16 devices (but no more than 8 alarm panels) connected to each port on an LNL-500 access panel.

Address

Each alarm panel is addressable, and has an address stored inside of it. Select the address that was set with DIP switches during alarm panel installation. Options fall in the range of 0 through 31.

Panel Type

Select the type of alarm panel you are configuring:

- LNL-1100 (input control module)
- LNL-1200 (output control module)

Add

Adds an alarm panel for an elevator reader.

Modify
Changes an alarm panel record.

Delete
Deletes an alarm panel record.

Help
Displays online assistance for this form.

Multiple Selection
If selected, two or more entries can be simultaneously checked in the listing window.

Close
Closes the Readers folder.

Elevator Hardware Form Procedures

Use the following procedures on this form.

Elevator Control Limits

Lenel controllers support up to 128 elevator floors as well as 128 inputs/outputs. To do this, the Single Reader Interface Module (LNL-1300), Alarm Input Control Module (LNL-1100), and Alarm Output Control Module (LNL-1200) are used.

The maximum number of elevator control levels (inputs/outputs) that can be created per segment is 255. This includes the “all floors always” and “no floors” values. All of these elevator control levels can be downloaded and used in Lenel hardware.

By using the Alarm Input Control Module (LNL-1100), the software can also track cardholder movement between floors.

Lenel Hardware	Type of Input or Output	Status
Single Reader Interface Module (LNL-1300)	Door Contact	Disabled
Single Reader Interface Module (LNL-1300)	REX	Disabled
Single Reader Interface Module (LNL-1300)	Door Strike Relay	Disabled
Single Reader Interface Module (LNL-1300)	Aux1	Enabled
Alarm Output Control Module (LNL-1200)	Outputs 1 - 16	Enabled for floor control
Alarm Input Control Module (LNL-1100)	Inputs 1 - 16	Enabled for floor tracking
Alarm Input Control Module (LNL-1100)	Outputs 1,2	Disabled

Standard Elevator Control Mode (No Floor Tracking)

Standard elevator control mode does NOT track cardholder usage of elevator controls.

Functionally, the sequence of events is this:

1. The cardholder swipes his card.
2. Buttons for the floors that the cardholder may access are illuminated for the duration of the strike time.
3. The cardholder presses the desired button.
4. The pressed button remains lit after the strike time, sending the elevator cab to the desired stop.

Configure the System for Standard Elevator Control Mode

1. Verify the access panel has elevator support. The **Elevator support** check box must be selected on the Options tab of the Access Panels folder.
2. On the General form, add a single interface type reader. Be sure to select the **Elevator** check box.
3. Click the Elevator Hardware tab. Although the elevator control feature uses standard alarm output control (LNL-1200) hardware, you must configure it using the Elevator Hardware form, NOT the Alarm Panels form.
4. In the listing window, select the entry for the reader you just added. You will now configure the alarm output panel(s) that this reader controls.
5. Click [Add].
6. Select the correct **Floors** value. Each panel can support up to 16 elevator cab control buttons, so you must configure the appropriate number of panels. For example, if you need to control 25 buttons in the elevator cab, you will need to configure two panels, one for buttons 1-16 and the second for the remaining buttons. There are 4 choices and they must be added in numerical order. In other words, for the first alarm output panel that you configure, you must select the value “floors 1-16.” The second panel must be assigned the value “floors 17-32,” etc.
7. Select the **Port**, **Address**, and **Panel Type** for the alarm output module. Standard elevator control mode requires alarm output control modules, so you must select the “LNL-1200 (Output)” **Panel Type** here.
8. Click [OK].
9. For each alarm output control module you add, 16 output relays are automatically added to the system for you; no additional configuration is required. A name is assigned to each relay based on the **Floors** selection you made. In other words, if you add an output panel to control floors 1-16, the relays will be labeled “Floor 1,” “Floor 2,” etc. These will be listed on the Alarm Outputs form of the Alarm Panels folder. Because for a given relay output the automatically assigned name might not match the actual floor numbers controlled, the application allows you to change the relay names and addresses on the Alarm Outputs form. Note that alarm panels, alarm inputs and linkages for elevator hardware aren’t displayed on the other forms in the folder.

   In the system tree, clicking on an elevator reader entry expands the entry to display all of the associated elevator control hardware. For each alarm output panel, you will see all of the outputs named as indicated on the alarm outputs form. This allows an Alarm Monitoring system operator to activate only a specific floor from his monitoring station. Alternatively, all floors controlled by the reader can be activated by right-clicking on the elevator reader entry and selecting **Open Doors** from the popup menu.

Floor Tracking Elevator Control Mode

Unlike Standard elevator control mode, floor tracking elevator control mode requires that you install both alarm input and alarm output control modules (LNL-1100 and LNL-1200). The floor tracking feature will not work if you do not have input control modules installed.

Configure the System for Floor Tracking Elevator Control Mode

To configure your system for floor tracking elevator control mode, you must do the following things in addition to the steps described in the procedure “Configure the System for Standard Elevator Control Mode”:

1. On the General form, you must select both the **Elevator** and **Track Floors** check boxes when configuring an elevator reader and want floor tracking.
2. On the Elevator Hardware form, you must add separate entries for the alarm input control modules in the same manner that you added entries for the output modules. In other words, you need entries for input modules and entries for output modules.

Functionality:

When floor tracking is enabled, the sequence of events is this:

1. The cardholder swipes his card.
2. No cab control buttons are illuminated. The reader will wait for up to the strike time for the cardholder to press a button. After the cardholder presses a button:
   - If the cardholder has access, the access cycle is completed and the button is lit, sending the cab to that floor. A single transaction is generated to the Alarm Monitoring system, indicating the identity of the cardholder and the floor pressed.
   - If the cardholder does not have access to the requested floor, no buttons will be illuminated. An “Access Denied” event will be generated to the Alarm Monitoring system, indicating the floor to which the cardholder attempted access.
   - Note that, in floor tracking elevator control mode, after ANY cab control button has been pressed, no other buttons can be pressed until another card swipe is performed.

In the Alarm Monitoring system, if an operator activates a relay output or selects the “Open Door” menu choice for the elevator reader, the cab control button will NOT be illuminated until a cab control button is selected.

Add an Alarm Panel for an Elevator Reader

1. On the General form, select (place a check mark beside) the elevator reader for which you wish to configure alarm panels.
2. Click [Add].
3. In the Floors drop-down list, select the range of outputs or inputs that this panel will control. You must configure these floors in order. Therefore, if the panel will control 30 floors, for example, you must add the entry for Floors 01 - 16 before you can add the entry for Floors 17 - 32.
4. Select the port for these inputs or outputs. Options include Ports 2 through 5 for an LNL-1000 and Ports 2 and 3 for an LNL-500.
5. Select the address that corresponds to this alarm panel you are configuring.
6. Select whether this is an output panel (LNL-1200) or an input panel (LNL-1100).
7. Click [OK].
8. Repeat steps 2-7 for each range of inputs or outputs you wish to configure.

Modify an Alarm Panel

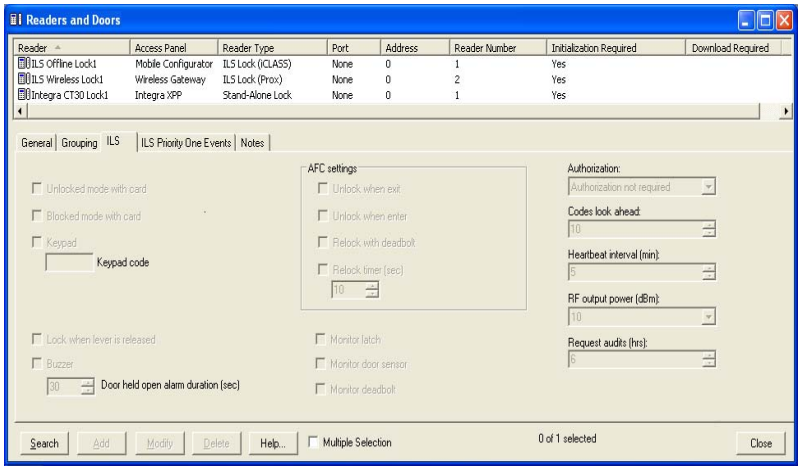
1. On the General form, select the entry you wish to change.
2. Click [Modify].
3. Make the changes you want.
4. Click [OK] to save the changes.

Delete an Alarm Panel

1. On the General form, select the entry you wish to delete. Note that, like adding panels, you must delete panels in sequence. In other words, you must delete the panel for Floors 17-32 before you can delete the panel for Floor 01-16.
2. Click [Delete].
3. Click [OK] to confirm the deletion.

ILS Form

Use this form to configure features that are unique to the ILS readers (locks).



IMPORTANT: To view this ILS form your system must have an ILS license.

Note: Depending on the lock type, some of the options on the ILS form may not be available. However, the AFC settings are available if these are configured in ILS System Options. For more information, refer to ILS Form on page 419. For information about the Alternative Fire Code, refer to the ILS Lock Operation User Guide.

Unlocked mode with card

When selected, allows the lock owner to put the door into Unlocked mode by swiping the card twice (double-dipping). The Unlocked mode allows free passage through the door; the door is unlocked (a card is not needed to unlock the door). To lock the door, and return to the previous mode of operation, the lock owner swipes the card twice again. For more information about lock owners, refer to Device Owner Form on page 124.

When double-dipping, the second swipe of the card must be performed within the allotted Held Open Time/Extended Open (or lock on release setting) before relock occurs after the first

presentation. For information on configuring Held Open and Extended Open times, refer to General Form on page 635.

Blocked mode with card

When selected, allows the lock to be put into the Blocked mode when a valid blocking card is presented.

Keypad

Select this option if the lock has a keypad and you want to use a keypad code and/or a cardholder PIN code.

Keypad code

If **Keypad** is enabled, then enter a code in this field. This keypad code will need to be entered to gain access to the door.

Lock when lever is released

When selected, if the cardholder is granted access, the lock will re-engage after the door handle is turned. When deselected, if the cardholder is granted access, then the lock will only re-engage after the specified **Strike Time**.

Buzzer

When selected, the buzzer will beep a low tone every two (2) seconds for the specified amount of time if the door is not closed before the Held Open Time expires. In addition, a visual indication will be provided via the LED.

Door held open alarm duration (sec)

The length of time the buzzer sounds when a Door Held Open alarm occurs. Select from 0 - 180 seconds with a default value of 30 seconds.

AFC settings

The settings in this section allow for Alternative Fire Code (AFC) functionality. AFC settings include:

- Unlock when exit
- Unlock when enter
- Relock with deadbolt
- Relock timer

These settings are only available if they are enabled in ILS System Options. For more information, refer to ILS Form on page 419. For more information about AFC, refer to the ILS Lock Operation User Guide.

Unlock when exit

When selected, causes the door to unlock, and remain unlocked when an individual uses the lever to exit the room. The lock will only relock when a valid card is used to relock the door or if either the **Relock timer** or **Relock with deadbolt** option is enabled, and that event occurs.

Unlock when enter

When selected, allows the lock to remain in an unlocked state after a valid card is used to open the door. The lock will only relock when a valid card is used to relock the door or if either the **Relock timer** option or **Relock with deadbolt** option is enabled, and that event occurs.

Relock with deadbolt

When selected, allows you to configure the lock to lock automatically when the deadbolt is engaged.

Relock timer (sec)

When selected, allows the relock timer to relock the door after a specified amount of time (seconds) after the door is unlocked. Configure the timer value in the **Relock timer** field. The relock timer can be configured from 1 - 5940 seconds (99 minutes).

Monitor latch

When selected, allows you use latch monitoring for the locks. The latch monitoring feature, used in conjunction with latch monitoring hardware, detects if the door is closed. The latch must be engaged in the strike for the door to indicate that it is closed. When latch monitoring hardware is present and enabled, the door events include the following:

- Granted Access Entry Made
- Granted Access No Entry Made

Because the locks only detect a change in state between door opened and door closed, the lock cannot detect if the hardware is not present or compromised. Therefore, if you receive an unusually large number of events such as “Access Granted No Entry Made,” this may indicate such a condition. If both **Monitor latch** and **Monitor door sensor** are enabled for the lock, the state of the door sensor takes precedence.

Monitor door sensor

When selected, allows you to use the door sensor for the locks. The door sensor feature, in conjunction with door sensor hardware, is used to physically secure the door. When door sensor hardware is present and enabled, the door events include the following:

- Granted Access Entry Made
- Granted Access No Entry Made

Because the locks only detect a change in state between door opened and door closed, the lock cannot detect if the hardware is not present or compromised. Therefore, if you receive an unusually large number of events such as “Access Granted No Entry Made,” this may indicate such a condition. If both **Monitor door sensor** and **Monitor latch** are enabled for the lock, the state of the door sensor takes precedence.

Monitor deadbolt

When selected, and the door is locked with the deadbolt engaged, only the lock owner will be granted access; the door will then unlock and the deadbolt will disengage when the door handle is turned. The lock ignores all scheduled mode changes while it is in the “privacy” state unless the reader mode is changed from OnGuard, the portable programmer, or a special purpose card (Emergency Lock, Emergency Unlock, or Blocking).

When deselected, and the door is locked with the deadbolt engaged, then anyone with a valid card will be granted access; the door will then unlock and the deadbolt will disengage when the door handle is turned.

Authorization

Authorizations are used to limit access when you have already created and implemented your locking plan. This allows you to create generic users in your locking plan before they are needed. For example, you might encode a generic visit card that only gives a visitor the authorization to enter Residence Hall A on a college campus, although in the locking plan, the generic visit card included all Residence Halls. To use only the locking plan to make access decisions, select “Authorization not required.” Otherwise, select one of the available authorization levels.

Codes look ahead

This option applies to all of the ILS locks within the system. It tells the lock how many future codes it should allow for each user with access to that lock. The allowed range is 5 - 99 with a default value of 10.

Heartbeat interval (min)

This is the delay time in minutes between "heartbeat" messages sent from the lock to OnGuard via the Wireless Gateway. It is used to notify OnGuard that the lock is still online. If OnGuard does not receive a heartbeat message within the specified time, then the lock is determined to be offline. The allowed range for the **Heartbeat interval** is 1 - 1440 minutes (24 hours) with a default value of 5 minutes.

If **Missed lock heartbeats** is greater than "1" for the Wireless Gateway, the lock will not go offline until the specified number of lock heartbeat messages are missed. Configuring a longer interval (more minutes) between heartbeats will extend lock battery life. For example, in comparison with the standard interval of every 5 minutes, if you configure the interval to every 1 minute, then the battery would last only about 20% of its standard lifetime. However, if you increase the interval to every 30 minutes, this would extend the battery life by 600%. If you reduce the heartbeat interval, this change will not take effect until the next heartbeat. Until then the lock will appear to be offline.

RF output power (dBm)

Specifies the RF (Radio Frequency) power for the lock. Choices include:

- 0 dBm
- 5 dBm
- 10 dBm
- 15 dBm

dBm refers to the power level of the signal strength expressed in decibels above 1 milliwatt.s.

Locks assigned to the Wireless Gateway typically use the **RF output power** configured for the Wireless Gateway. However, you may need to increase the power level for locks placed at a greater distance from the Wireless Gateway to optimize their signal strength. If you modify **RF output power**, in order for this change to take effect, you must update the lock using the Mobile Configurator.

Request audits (hrs)

Specifies the time interval at which incremental events are retrieved from the ILS wireless lock. Incremental events are those events stored in the lock that have not been sent to OnGuard. At each interval, a request is placed on the queue to retrieve the incremental events on the next heartbeat. The allowed range for the **Request audits** interval is 1 - 255 hours with a default value of every six (6) hours. However, the value in **Request audits** must be greater than the heartbeat time.

Events retrieved during the Request audits interval are obtained independently of the heartbeat and priority one schedules. You can also manually request audits in Alarm Monitoring. For more information, refer to Retrieve Wireless Lock Events in the Alarm Monitoring User Guide.

Add

Adds a reader to the system.

Modify

Changes a reader entry.

Delete

Removes the selected reader(s).

Help
Displays pertinent help information onscreen.

Multiple Selection
If selected, two or more reader entries can be simultaneously checked in the listing window.

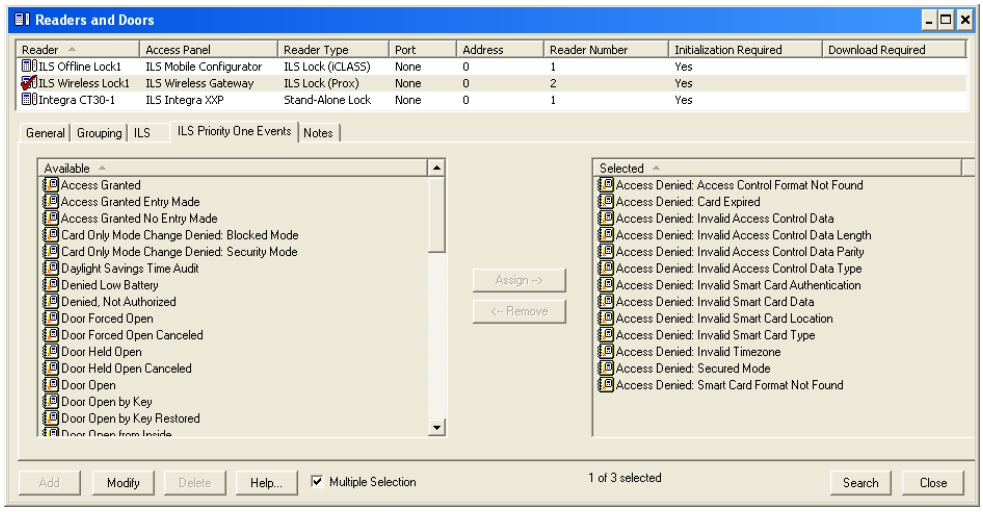
Close
Closes the Readers and Doors folder.

ILS Form Procedures

To read how to configure an ILS locking system, refer to Appendix K: Lenel ILS (Integrated Locking Solutions) on page 1473.

ILS Priority One Events Form

Use this form to specify up to 20 events as priority one events on a lock-by-lock basis. To configure priority one events on a system-wide basis, use the ILS Priority One Events form in the Alarm Configuration folder. By default, all ILS wireless locks are initially configured with the system priority one events. For more information, refer to ILS Priority One Events Form on page 879.



IMPORTANT: To view this ILS form your system must have an ILS license.

Note: Depending on the lock type, some of the options on the ILS form may not be available.

Available
Lists all ILS wireless lock events.

Selected
Lists ILS wireless lock events assigned as priority one events. Priority one events are sent to Alarm Monitoring, filtering out all other lock events.

Assign
Click to move selected events to the list of priority one events. Up to 20 events can be assigned as priority one.

Remove
Click to remove events from the list of priority one events.

Modify
Used to change an event's configuration.

Help
Displays online assistance for this form.

Search
Displayed in view mode on every form in the Readers and Doors folder. This button is used to search for and list existing readers that meet the specified reader group search criteria.

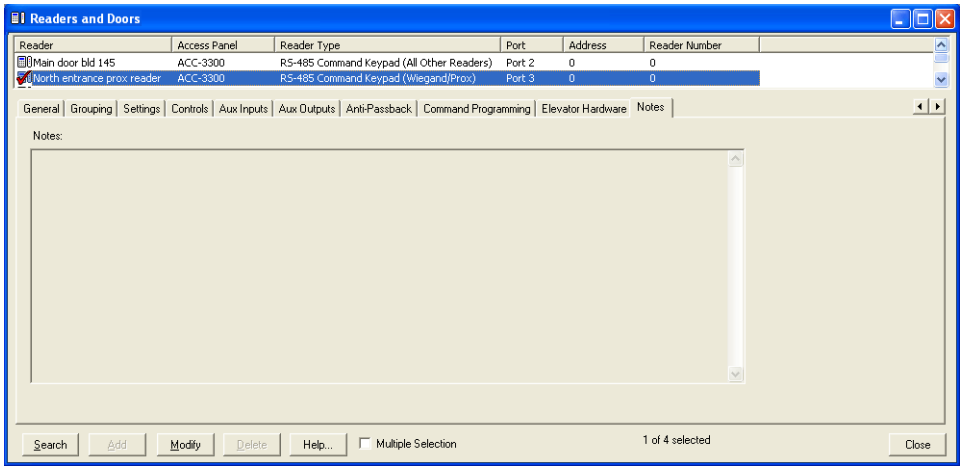
Close
Closes the Readers and Doors folder.

ILS Priority One Events Form Procedures

For instructions on how to configure an ILS locking system, refer to Appendix K: Lenel ILS (Integrated Locking Solutions) on page 1473..

Notes Form

This form is used to enter information about a reader, which can then be displayed in Alarm Monitoring.



Notes
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide.

Modify
Used to configure reader settings.

Help
Displays online assistance for this form.

Multiple Selection
If selected, two or more entries can be simultaneously checked in the listing window.

Close
Closes the Readers and Doors folder.

Notes Form Procedures

Use the following procedures on this form.

Enter Reader Notes

1. From the ***Access Control*** menu, select ***Readers and Doors***. The Readers and Doors folder opens.
2. Click the Notes tab.
3. In the listing window, select the entry you want to edit.
4. Click [Modify].
5. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
6. Click [OK].

CHAPTER 29

Alarm Panels Folder

The Alarm Panels folder contains forms with which you can:

- Name individual alarm panels in the software
- Specify setup parameters, including the alarm panel type and its panel address
- Name and describe each of the alarm panel's inputs and outputs
- Specify the output(s) to be triggered by a specific input

The folder contains four forms: the Alarm Panels form, the Alarm Inputs form, the Alarm Outputs form, and the Input/Output Local Linkage form.

The Alarm Panels folder is displayed by selecting ***Alarm Panels*** from the ***Access Control*** menu, or by selecting the Alarm Panels tool bar button.

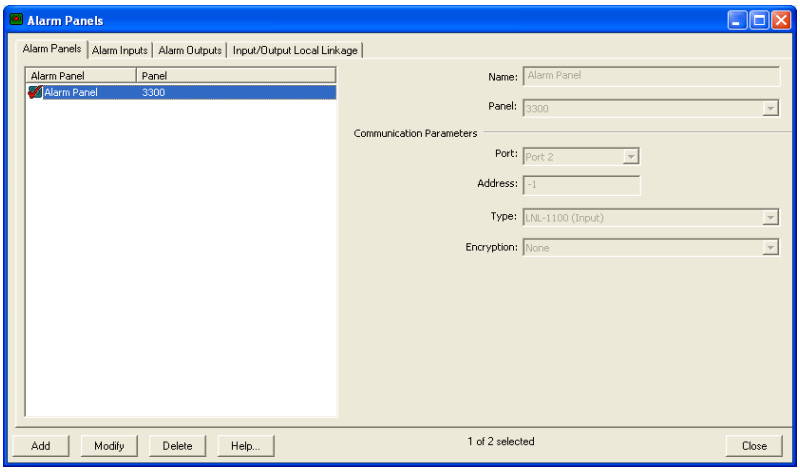
Toolbar Shortcut

Alarm Panels Form

This form is used to:

- Name individual alarm panels in the software
- Specify setup parameters, including the alarm panel type and its panel address
- CASI alarm panels are configured automatically when a CASI access panel is added and/or an input/output device extension board is assigned to a CASI access panel slot. For more information, refer to NGP Form (Slots) on page 1547.

IMPORTANT: A full panel download may be required the first time a downstream device (alarm panel) is added to an LNL-2210 panel or when the only downstream device assigned to that panel is deleted.



Listing window

Lists currently defined alarm panels and the panels associated with each.

Name

Enter a unique name for the alarm panel. This name will appear on other forms in this folders, and elsewhere in the system.

Panel

Select the panel to which the alarm panel is connected. Depending on the panel selected the fields options on this screen will change.

Port

For Lenel Alarm Panels only. Select the choice that indicates to which of the panel ports this alarm panel is attached. Each panel has communication ports used for field hardware devices such as readers or alarm panels. The LNL-500 can have from 1 to 2 ports (Ports 2-3) depending on the configuration of the panel. The LNL-1000 and the LNL-2000 can have from 2 to 4 ports (Ports 2-5) depending on the configuration of the panel.

For the LNL-500, 2- and/or 4-wire communication can be used, depending upon the configuration. There can be up to 16 downstream devices (alarm panels and readers modules).

For the LNL-1000 and LNL-2000, 2- and/or 4-wire communication can be used, depending upon the configuration. There can be up to 32 downstream devices (alarm panels and readers modules) connected to each port on a panel.

For the LNL-2210, 2-wire communication can be used. Depending upon the configuration, if one on-board reader is configured, there can be up to 8 downstream devices (alarm panels and readers modules). If dual interface readers are used, there can be up to 16 off-board readers. However, if a second on-board reader is configured, downstream devices are NOT supported.

Address

For Lenel Alarm Panels only. Select the number that corresponds to the DIP switch settings for addressing, on the alarm panel. You can choose a value in the range of 0 through 31.

This field displays only for alarm panels added to access control panels. If you are adding an alarm panel to any other hardware, this field does not display.

Type

For Lenel and Visonic Alarm Panels only. Select the type of alarm panel. Choices will differ depending on whether the **Panel** is an LNL-1000, LNL-2000, LNL-500, fire panel, or a Visonic SpiderAlert Personal Safety Device.

Encryption

For Lenel Alarm Panels only. This field is used for configuring downstream encryption. This field is enabled only if the following conditions are met:

- The panel type is an LNL-1100 or LNL-1200.
- The reader is connected to an LNL-2220 or LNL-3300 access panel.
- Host and downstream encryption are both enabled for the specific access panel.

Alarm Panel ID

For Visonic Alarm Panels only. This field displays only for alarm panels added to hardware devices that are not access control panels.

If configuring alarm panels for personal safety devices:

- For Visonic SpiderAlert devices, Alarm Panel ID is displayed as a two digit hexadecimal number in the range 00 - FF (0 - 255 decimal). This is because when these devices are shipped from the factory, this is how their IDs are indicated. Also, this is format that Visonic uses to refer to these IDs.
- For Generic Personal Safety devices, Alarm Panel ID must be a number between 1 and 255.

ID

For NGP Alarm Panels only. Enter the alarm panel ID as displayed on your NGP panel. The ID acts as a unique identifier for the hardware.

Serial Number

For NGP Alarm Panels only. Enter the Serial Number as displayed on your NGP panel.

Model

For NGP Alarm Panels only. If available, select the Model of the NGP panel.

Number of Inputs

For NGP Alarm Panels only. Lists the number of inputs the NGP panel is capable of having.

Number of Outputs

For NGP Alarm Panels only. Select the number of outputs the NGP panel will use.

Area

For NGP Alarm Panels only. Select the pre-defined area that the NGP alarm panel will use.

Add

Adds an alarm panel entry.

Modify

Changes an alarm panel entry.

Delete

Removes an alarm panel entry.

Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the Alarm Panels folder.

Alarm Panels Form Procedures

Use the following procedures on this form.

Add an Alarm Panel

1. Select ***Alarm Panels*** from the ***Access Control*** menu.
2. Click [Add].
3. In the **Alarm Panel Name** field, type a unique, descriptive name for the alarm panel.
4. Select the panel to which the alarm panel is connected.
5. Complete the Communication Parameters section, indicating the port and address used to connect the alarm panel to the access panel and the type of alarm panel used.

Note: The **Address** spin buttons display only if you are adding an alarm panel to an access control panel.

6. Click [OK].

Modify an Alarm Panel

1. In the listing window, select the name of the alarm panel you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an Alarm Panel

1. In the listing window, select the name of the alarm panel you wish to delete.
2. Click [Delete].
3. Click [OK].

Add a Visonic Bus Device

1. Select ***Alarm Panels*** from the ***Access Control*** menu, or click the icon to display the Alarm Panels form.
2. Click [Add].
3. In the **Alarm Panel Name** field, type a unique, descriptive name that is no more than 32 characters long.

4. In the **Panel** field, select a panel from the drop-down list. Depending on the panel selected, the **Port** field may become disabled.

Note: These panels must be added on the Personal Safety Panels form in the Personal Safety devices folder before they will appear in the **Panel** drop-down list.

5. Select a value for the **Port** (if enabled) from the drop-down list.
6. Select a value for the **Type** from the drop-down list.
7. In the **Alarm Panel ID** field, enter the device's two-digit hexadecimal ID.
8. Click [OK].

Modify a Visonic Bus Device

1. Select ***Alarm Panels*** from the ***Access Control*** menu, or click the icon to display the Alarm Panels form.
2. In the listing window, select the entry you want to modify. A selected entry has a red checkmark over the icon.
3. Click [Modify].
4. The **Alarm Panel Name** field is the only field that is allowed to be changed. Make any changes to the name that you want. (To change the **Type** or **Alarm Panel ID**, you must delete the alarm panel, then add a new one.)
5. Click [OK].

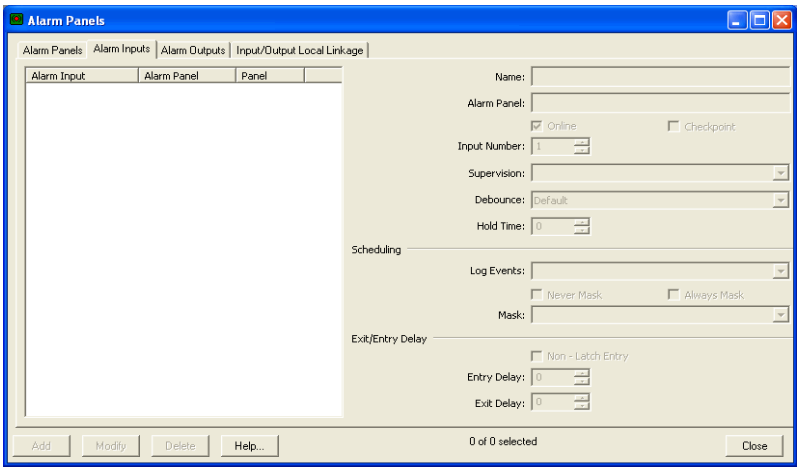
Delete a Visonic Bus Device

1. Select ***Alarm Panels*** from the ***Access Control*** menu, or click the icon to display the Alarm Panels form.
2. In the listing window, select the entry you want to delete. A selected entry has a red checkmark over the icon.
3. Click [Delete].
4. Click [OK].

Alarm Inputs Form

This form is used to:

- Name an alarm panel's individual alarm inputs
- Specify setup parameters, including the input number on the panel, and when to mask the input (if ever)
- If the alarm panel is digital, identify the DSS address for the input



Listing window

In view mode, lists currently defined alarm inputs, and the alarm panels and panels associated with each. In modify mode, lists currently defined alarm panels and the panels associated with each.

Name

Enter a name for the alarm input. This name will also appear on the Input/Output Local Linkage form.

Alarm Panel

For NGP Alarm Panels only. Lists the alarm panel selected.

LCD Name

For NGP Alarm Panels only. The name as it will appear on the LCD keypad. This field is not available for CASI alarm panels.

Supervision

Select a supervision and normally open/closed setting from the drop-down list. Choices in the drop-down list are based on the EOL tables. There are four built-in tables and up to four custom tables that can be configured by the user. For more information, refer to Chapter 39: EOL Tables Folder on page 819. The four built in tables are:

- Default Supervision, Normally Closed
- Default Supervision, Normally Open
- Not Supervised, Normally Closed
- Not Supervised, Normally Open

Notes: You can configure up to eight (8) different settings (EOL resistor tables) *per* panel.

NGP-1100 alarm panels support up to four (4) different EOL resistor tables *per* panel.

Each auxiliary input can be individually wired for either supervised or unsupervised activity. An unsupervised input is an unprotected, low security input. Someone can short-circuit the connection between the auxiliary input and the device controlled by the input, thereby defeating the circuit. Although the device may trigger an alarm condition in such a situation, the auxiliary input will not be aware of it.

By contrast, a supervised input's circuit is equipped with resistors. Subtle changes in the voltage on the circuit can be detected to determine whether someone has tampered with the wiring. For this reason, supervised inputs are high security.

Debounce

For Lenel hardware only. Debounce is the amount of time that an input must change state in order for that change to be considered a logical change of state.

There are six levels of debounce (1-6). These are relative levels with 1 being the lowest (shortest) and 6 being the highest (longest). It is up to the hardware interface to map these values to hardware specific values, as well as to map the "Default" option to a hardware specific value. The Lenel hardware interface maps these values to:

- 1 - Lenel value of two scans, ~33 ms (default for REX)
- 2 - Lenel value of four scans, ~67 ms
- 3 - Lenel value of six scans, ~100 ms (default for door contact and alarm and reader aux inputs)
- 4 - Lenel value of nine scans, ~150 ms
- 5 - Lenel value of 12 scans, ~200 ms
- 6 - Lenel value of 15 scans, ~250 ms

It is recommended that the debounce time should not be changed and left at the default setting of "Default."

Point Type

For NGP-2220i and 3320i Alarm Panels only. Select the type of sensor and/or the type of monitoring to be used with this point. Identifies an input point on the perimeter of an area. Available selections include many pre-defined types plus custom types 80-99 that can be set up manually. For more information, refer to Input Point-Type Reference on page 1578.

Notes: If "Work late" is selected, this feature will be available for the alarm input. If an input point such as a work late motion detector is activated because area occupants are working late, the work late condition will delay the scheduled closing time.

Scheduled closing time delay: Select the delay interval from the Areas > Arming/ Disarming sub-tab > **Work late input** drop-down.

Note: Non-intrusion panels are pre-configured to "Standard."

Log Events

Select the timezone during which events originating at this alarm input are to be logged by the system. If this field is left blank, all events from this input will be recorded.

Online

If selected, indicates that the input is online and in communication with the alarm panel. If NOT selected, the input will not be monitored by the panel, thus preventing events from reporting back to the panel. This field may be useful for initial system configuration if the alarm input has not yet been installed.

Checkpoint

Select this check box to designate the device as a checkpoint. This device will be listed along with all other devices that have this check box selected when the **Only show devices marked as checkpoints** check box is selected when adding a guard tour.

Input Number

Select the number that matches the input's number on the panel. The value will be in the range of 1 through 16.

Hold Time

When an input goes active and is restored, enter the amount of time (in seconds) to wait until reporting the input as restored. If the input goes active again within the hold time, a change of state is not reported, but just remains as active.

This feature is useful when there is no advantage to log the specific number of times a point is tripped after the initial event. For example, if a motion detector is tripped into active, the state remains there for the hold time after the last motion event is detected. You can enter a value of 0 to 15 seconds.

Mask

Select Mask option. Choices are:

- **Always** - Select if the alarms from this input are never to be reported to alarm monitoring or logged to the database.
- **Never** - Select if the alarms from this input are always to be reported to alarm monitoring or logged to the database.
- **Weekend** - Select to mask the alarm inputs on non-workdays. When the timezone in this field is active, events from this input will not be reported to alarm monitoring or recorded to the database.
- **Workday** - Select to mask the alarm inputs on workdays. When the timezone in this field is active, events from this input will not be reported to alarm monitoring or recorded to the database.

Exit /Entry Delay

Includes the **Non-Latch Entry**, **Entry Delay**, and **Exit Delay** fields.

Non-Latch Entry

Used in conjunction with the **Entry Delay** field.

When checked, the **Entry Delay** being configured will be a Non-Latch entry delay.

Entry Delay

Used in conjunction with the **Non-Latch Entry** field.

- If the **Non-Latch Entry** check box is selected (i.e. non-latched mode), when the alarm input is active the alarm will NOT be reported until the **Entry Delay** time expires. The alarm will only be reported if the input is still active at the end of the specified delay. Application: false alarm prevention such as invalid motion detector reads.
- If the **Non-Latch Entry** check box is not selected (i.e. latched mode), when the alarm input is active the alarm WILL be reported unless the input is masked (either automatically through the software or manually via a keypad) within the specified delay after the alarm input goes active. Application: valid access to a room with motion detectors.

Exit Delay

Specifies the delay, in seconds, for the alarm input to switch from a masked state to an unmasked state. You can choose a value in the range of 0 through 32767. When an alarm input is unmasked, active alarms will NOT be reported until the **Exit Delay** expires. Application: securing a room upon exit (such as activating motion detectors).

Area
For NGP Alarm Panels only. The area that this point is associated with.

Buffer Area
For NGP Alarm Panels only. Where a door adjoins two areas, select the second area here. The system will apply appropriate entry/exit delays whenever only one of the two areas is fully armed.

Zone Number
For NGP-2220i and 3320i Alarm Panels only. The reporting zone for the area that this point is associated with. Enter a zone numbers from 0 - 998. The default value is 0. All zone numbers except the default value (zero) must be unique within a given area.

Add
Used to add an alarm input entry.

Modify
Used to change an alarm input entry.

Delete
Used to remove an alarm input entry.

Help
Displays online assistance for this form.

Close
Closes the Alarm Panels folder.

Alarm Inputs Form Procedures

Use the following procedures on this form.

Add an Alarm Input

1. Click [Add].
2. In the listing window, select the name of the alarm panel for which you're adding this input.
3. In the **Name** field, type a unique, descriptive name for this input.
4. Indicate whether the input should be **Online** and if you want it to be configured as a **Checkpoint**.
5. Select a supervision and normally open/closed setting from the **Supervision** drop-down list.
6. It is recommended that the debounce time should not be changed and left at the default setting of "Default." However, if you want to change this value, select an option from the **Debounce** drop-down list. Debounce is the amount of time that an input must change state in order for that change to be considered a logical change of state. There are six levels of debounce (1-6). These are relative levels with 1 being the lowest (shortest) and 6 being the highest (longest). It is up to the hardware interface to map these values to hardware specific values, as well as to map the "Default" option to a hardware specific value. The Lenel hardware interface maps these values to:
   - 1 - Lenel value of two scans, ~33 ms (default for REX)
   - 2 - Lenel value of four scans, ~67 ms

- 3 - Lenel value of six scans, ~100 ms (default for door contact and alarm and reader aux inputs)
- 4 - Lenel value of nine scans, ~150 ms
- 5 - Lenel value of 12 scans, ~200 ms
- 6 - Lenel value of 15 scans, ~250 ms

Note: The **Debounce** field is available for Lenel hardware only.

7. Specify the **Input Number**.
8. Specify a **Hold Time**. When an input goes active and is restored, enter the amount of time (in seconds) to wait until reporting the input as restored. If the input goes active again within the hold time, a change of state is not reported, but just remains as active.
9. Select the timezone, if any, during which to log events associated with this input.
10. If you wish to mask this input sometimes or always, choose the appropriate setting in the Mask Configuration section.
11. Indicate the **Entry Delay** or **Exit Delay** time. If **Entry Delay** is specified, indicate whether or not to use **Non-Latch Entry** mode.
12. Click [OK].

Modify an Alarm Input

1. In the listing window, select the name of the alarm input you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

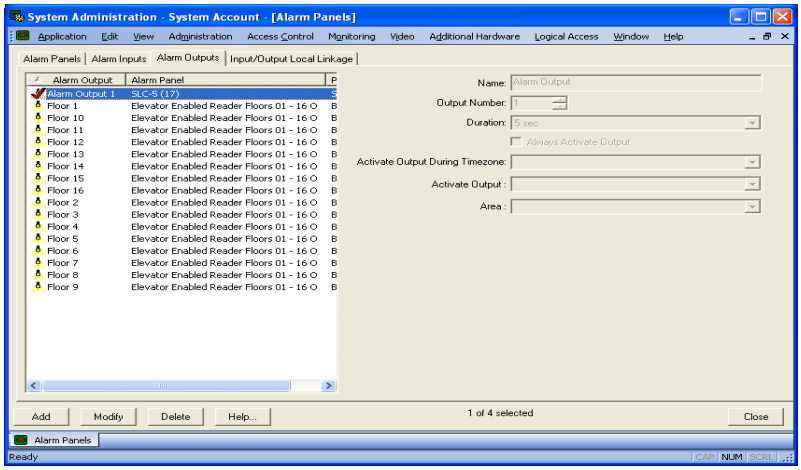
Delete an Alarm Input

1. In the listing window, select the name of the alarm input you wish to delete.
2. Click [Delete].
3. Click [OK].

Alarm Outputs Form

This form is used to:

- Name an alarm panel's individual alarm outputs
- Specify setup parameters, including the output number on the panel, when to activate it, and for how long
- For elevator control relay output: Change the name and/or output number for an elevator control relay output
- For CASI alarm output: Change the name, output number, and/or specify when to activate it, and for how long



Listing window

In view mode, lists currently defined alarm outputs, and the alarm panels and panels associated with each. In modify mode, lists currently defined alarm panels and the panels associated with each.

Name

Enter a name of 32 characters or less for the output. The name you use will also appear on the Input/Output Local Linkage form as well as in Alarm Monitoring.

Output Number

Select the number that is one less than the RLY# on the Relay Output Module to which the relay is attached. The value will be in the range of 0 - 15.

Duration

Specifies how long the relay will be active when it is pulsed from either a user (operator) action or from the execution of a local I/O function list. The output will remain on for the defined duration, unless another function list, timezone control schedule, or operator action deactivates the output. Enter the time in seconds. The maximum value is 32,767 for Lenel panels. This field is not available for elevator control relay outputs.

Always Activate Output

If this check box is selected, the output will be always activated. This field is not available for elevator control relay outputs or CASI outputs.

Activate Output During Timezone

If you wish to activate the relay for specific durations, choose the timezone that spans the indicated intervals. Available choices are the currently defined timezones. This field is not available for elevator control relay outputs.

Activate Output

When the main control panel goes into the specified alarm state (In Alarm, Siren, or Area Local Alarm), the output is activated. If “Area Local Siren” is selected, the **Area** drop-down is enabled. This field is not available for CASI panels.

Note: An output state controlled by a local function takes precedence over an output state configured for the alarm panel.

Area
Specifies the area where the local siren is activated. Choose from all areas assigned to this access panel. This field is not available for CASI panels.

Add
Used to add an alarm output entry.

Modify
Used to change an alarm output entry.

Delete
Used to remove an alarm output entry.

Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as "1 of 42 selected"). In modify mode, indicates the current operation, such as "Modify Mode."

Close
Closes the Alarm Panels folder.

Alarm Outputs Form Procedures

Use the following procedures on this form.

Add an Alarm Output

1. Click [Add].
2. In the listing window, select the name of the alarm panel for which you're adding this output.
3. In the **Name** field, type a unique, descriptive name for this output.
4. Choose the output's ID number, when it will be active, and for how long it will be triggered.
5. Click [OK].

Modify an Alarm Output

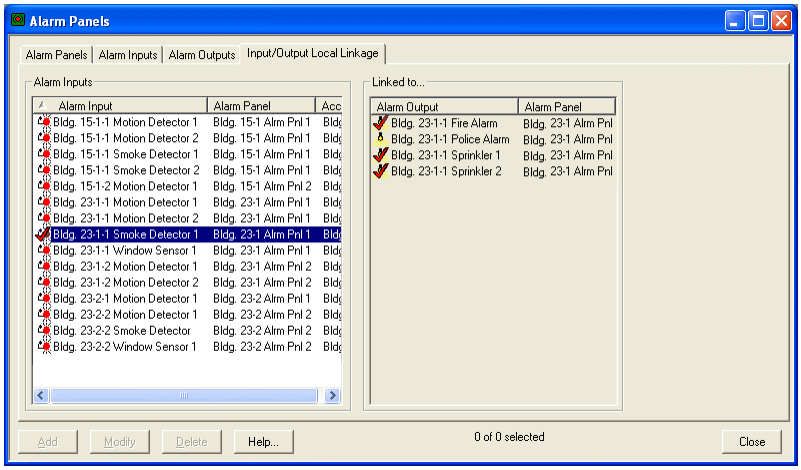
1. In the listing window, select the name of the alarm output you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an Alarm Output

1. In the listing window, select the name of the alarm output you wish to delete.
2. Click [Delete].
3. Click [OK].

Input/Output Local Linkage Form

This form is used to specify one or more output(s) to be triggered by a specific input.



Alarm Inputs

The window lists all alarm inputs, and the alarm panel and panel with which each is associated.

Linked to

Lists currently defined alarm outputs and the alarm panel with which each is associated. In this window, select one or more alarm outputs to be linked to the selected alarm input.

Add

This button is not used.

Modify

Used to link one or more alarm output(s) to an alarm input.

Delete

This button is not used.

Help

Displays online assistance for this form.

Mode

In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close

Closes the Alarm Panels folder.

Input/Output Local Linkage Form Procedures

Use the following procedures on this form.

Create an Input-to-Output Link

1. In the listing window, select the name of the alarm input to be linked to one or more outputs.
2. Click [Modify].
3. In the **Linked to** field, choose the alarm output(s) that will be linked to the selected input. To select an output, click on its icon. A selected output has a checkmark on its icon.

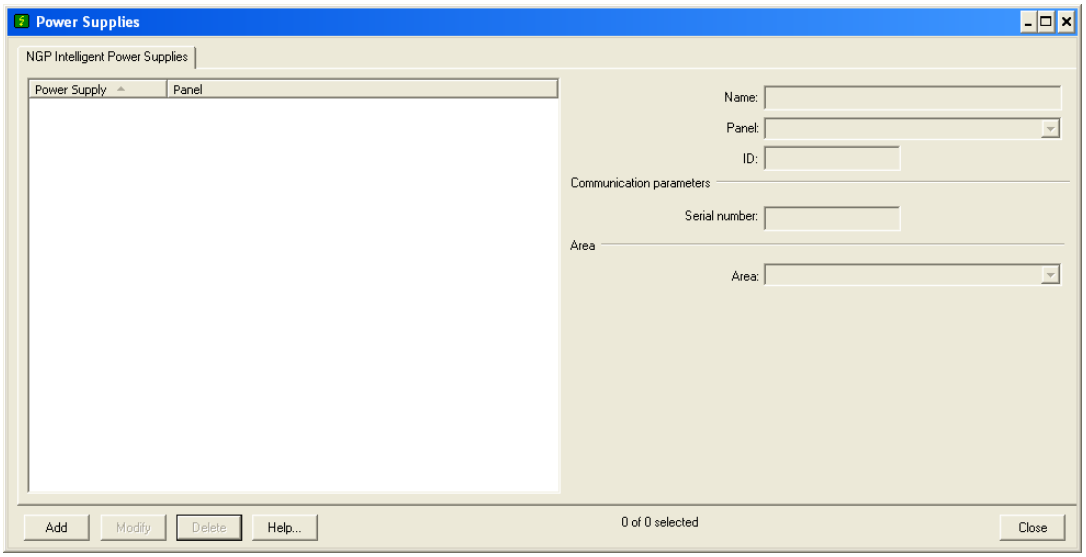
   You can link multiple outputs to a single input.
4. Click [OK].

CHAPTER 30

Power Supplies

The Power Supplies folder allows you to add an intelligent power supply board to your NGP panel.

The power supply board communicates with the NGP main controller on its module communication bus (SNAPP), allowing remote diagnostics of the power supply.



Name

Enter a name for the power supply. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Panel

Select the panel that the power supply will be associated to.

ID

The ID is automatically generated.

Serial number

Also known as the host address. Enter the serial number of the specific power supply. This allows the software to identify each panel. The serial number is typically a 5-digit number printed on a small sticker on the circuit board. For the Universal series, the serial number is the last 6 digits of the serial number printed on the sticker on the circuit board.

Area

Select the area that the power supply will be associated to.

Power Supplies Procedures

For more information, refer to Add an NGP Power Supply on page 1575.

CHAPTER 31

Dialup Configuration Folder

The Dialup Configuration folder contains the Modem Settings form with which you can:

- Configure dialup modems that can be used to communicate with access panels.
- Identify the workstations modems are attached to.

This folder is displayed by selecting ***Modems*** from the ***Access Control*** menu, or by selecting the Modems toolbar button.

Toolbar Shortcut

Modem Settings Form

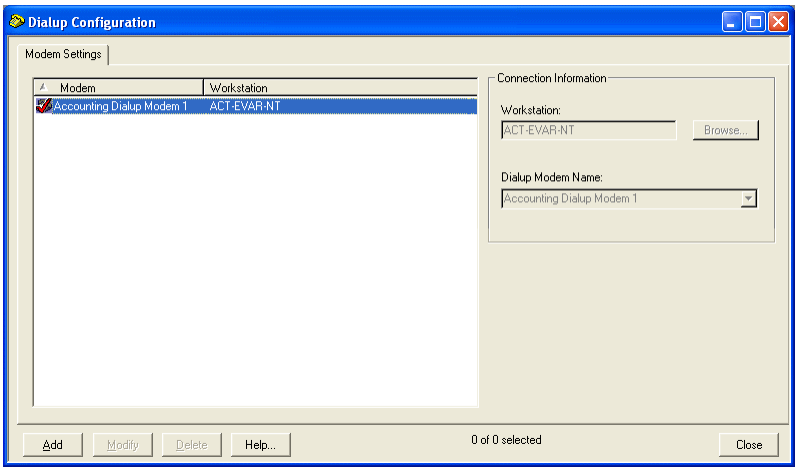
This form is used to configure dialup modems that can be used to communicate with access panels.

Notes: The more modems you have the better, but you can't define more modems than the current number of access panels.

Ideally, you should define a different modem for each access panel.

You should have at least as many phone lines (numbers) as modems.

Multiple access panels can use the same modem. This arrangement is referred to as *modem sharing*.



Listing window

Lists all currently defined modems.

Connection Information

Contains the [Browse] button, and the **Workstation** and **Dialup Modem Name** fields.

Workstation

Identifies the workstation to which the modem is attached. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Browse the network for the appropriate workstation.

Dialup Modem Name

Name of the dialup modem. The options available in this drop-down list are available after you set up a host modem.

Add

Used to add dialup modem record.

Modify

Used to change a dialup modem record.

Delete

Used to remove a dialup modem record.

Help

Displays online assistance for this form.

Mode

In view mode, indicates the record number of the selected dialup modem, and the current total number of dialup modems, for example, "1 of 5 selected".

Close

Closes the Dialup Configuration folder.

Host Modems Supported

Host modems are set up as TAPI modems in windows. This allows more brands and types of modems to be supported on the host side. Below are a few of the modems that have been used successfully on the host side:

- Practical Peripherals 336 MiniTower (Model 5913US)
- USRobotics 56k (Model 0459)
- Practical Peripherals PM144MT II (Model PM0438S)
- Practical Peripherals PM288MT II V.34 (Model PM0438VS)
- Practical Peripherals PM144MT II (Model 5615US)

Modem Procedures For Lenel Access Panels

Use the following procedures on this form.

Set Up a Lenel Host Modem

1. Connect the modem to the Com port of the workstation. Verify the modem has power and is connected to a phone line.
2. Click the Start button and select ***Settings*** > ***Control Panel*** > ***Phone and Modem Options***.
3. Click the Modems tab.
4. Windows XP should automatically detect a new device. Follow the Install New Modem wizard to install your modem. If you need the drive file for the modem, it should be located on the software included with the modem or possibly on the manufacturer's website.

Note: If Windows XP detects a standard modem you need to manually add the modem.

5. Select the modem and click [Add].

Add a Dialup Modem Record

Notes: If you are configuring dialup configuration from another machine that the modem is not on, the Communication Server must be running on the specified **Workstation** at the time the modem is selected in the **Dialup Modem Name** field, or an error message will be displayed and no choices will be listed.

If you are on the same machine that the modem is on then you do not need to have the Communication Server running on your machine.

1. In the System Administration application, display the Modem Settings form by selecting ***Modems*** from the ***Access Control*** menu.
2. Click [Add].
3. Enter the workstation name that the modem will be connected to. It's best to select the workstation using the [Browse] button.

Note: You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

4. Enter or select the **Dialup Modem Name**.

   A list of modems displays if:

   - You are using the computer that you are configuring a modem for and the modem is attached
   - You are using a computer that does not have the modem attached, but the selected **Workstation** with a modem attached is running the Communication Server

   A list of modems will not display if:

   - The specified **Workstation** is not running the Communication Server application
   - The specified **Workstation** has no TAPI devices configured on it/does not have a modem attached

5. Click [OK].

Connect a Modem to a Lenel Access Panel

1. Connect the modem to the port 1of the access panel. Be sure to use an RS-232 wire with a 5 pin connection.
2. Verify the dip switch settings on the modem are correct. Refer to the hardware documentation for wire diagrams and other dip switch settings.
3. Verify the modem has power and is connected to a phone line.

Set up a Lenel Access Panel for Dialup Connection

Notes: The Address field on the Location sub-tab of the Access Panel form must be set to 1 for any and all access panels that use a dial up connection.

If you are using a dial up connection as the primary connection for an LNL-2000 then the secondary connection must also be a dial up connection.

1. Select ***Access Panels*** from the ***Access Control*** menu.
2. Select the correct Access Panel form.
3. Click the Location tab. Verify the Address field is set to 1.
4. Click the Connection tab.
5. Click [Add].
6. If you are working with a segmented system, select the appropriate segment and click [OK].
7. Select the **Dialup** radio button.
8. Select the Modem from the drop-down list.
9. Enter the Host number which is the phone number used to connect the modem to the workstation.
10. Enter the Panel number which is the phone number used to connect to the access panel.
11. (Optional) Select the timezone when the access panel will connect to the modem. Select ***Timezones*** from the ***Access Control*** menu to configure timezones. For more information refer to the Timezones Folder chapter.
12. (Optional) Enter a value for the Dial-back after field if you want to download information after a certain number of events occur.

CHAPTER 32

Timezones Folder

The Timezones folder contains forms with which you can:

- Identify specific dates as holidays, enable holidays to repeat yearly, and assign a type to each
- Create timezones - groups of time/day intervals
- For a given reader, specify different modes of operation for the beginning and end of a particular timezone

The folder contains three forms: the Holidays form, the Timezones form, and the Timezone/Reader Modes form.

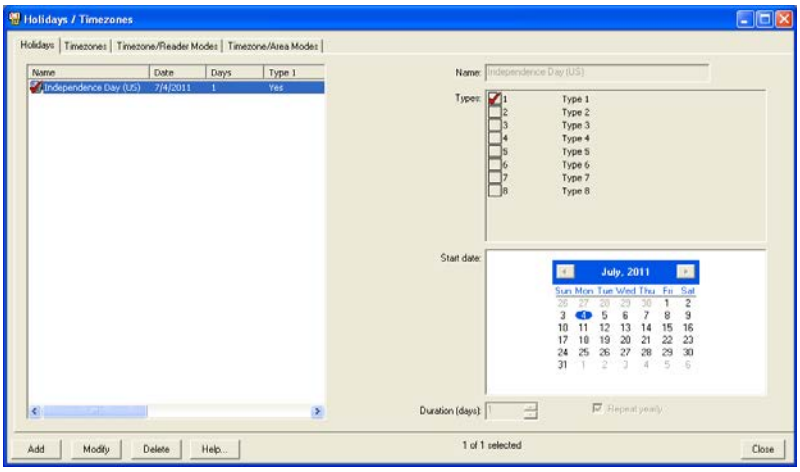
The Timezones folder is displayed by selecting ***Timezones*** from the ***Access Control*** menu, or by selecting the Timezones toolbar button.

Toolbar Shortcut

Holidays Form

This form is used to define specific dates (or ranges of specific dates) as holidays, enable holidays to repeat yearly, and categorize each holiday into any of 8 types, or into multiple types. In addition, holidays may be configured to repeat yearly.

Hardware Dependencies: Lenel access panels support up to 255 holidays. If your system contains both Lenel and non-Lenel access panels, you should consider using segmentation in order to avoid operator entry error and to take advantage of the extended performance features of the LNL-1000 access panel. If your system uses segmentation, your System Administrator determines the maximum number of holidays allowed per segment.



Listing window

Lists currently defined holidays, arranged in rows and columns. Each column represents a field that is included in a holiday entry. Click on a column heading to arrange the contents of the listing window by that field.

- **Name** – name of the holiday, as defined in the Description field
- **Date** – date of the holiday, in MMM DD, YY (DAY) format
- **Days** – the number of days that the holiday will be in effect, as defined in the Holiday Duration section
- **Type 1** through **Type 8** – displays “Yes” or “No” to indicate whether or not the holiday is of that Type

You can resize the width of a column for better visibility. To do this, position the mouse pointer over the boundary of two column headings. Then click and drag to resize the column.

Name

Indicates the name of the holiday, and corresponds to the **Name** field in the listing window. You can enter a description of no more than 32 characters.

Types

Indicates that this holiday is of the selected type(s). A holiday can be of Type 1, 2, 3, 4, 5, 6, 7, 8, more than one of these, or all of these. At least one type MUST be selected for a holiday, or the holiday will not be active within the access panel. Lenel access panels can accept all 8 holiday types. Other access panels will recognize only holiday types 1 and 2.

Holiday types enable you to create different holiday schedules for different types of cardholders. You may, for example, define as one type all holidays scheduled for employees, and define holidays for contractors and vendors to be of another type. This would offer you the flexibility to configure different holiday schedules for different types of people. You can change the name of the Type by right-clicking on it.

Start Date

Select a start date on the calendar. To select a month, click on the and navigation buttons. You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it. Navigate to a year by clicking on the displayed year to access the year spin buttons, and then choose the year that you want. Once you have selected a month and a year, click on the day you want the holiday to start on.

Duration (days)
Select the number days that you want the selected holiday to last.

Repeat yearly
Specifies that a holiday is to repeat every year. When **Repeat yearly** is selected, OnGuard automatically recalculates the holiday's year during panel downloads. Linkage server must be running in order to update holidays.

Add
Used to add a holiday entry.

Modify
Used to change a holiday entry.

Delete
Used to remove a holiday entry.

Help
Displays pertinent online help information.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the Timezones folder.

Holidays Form Procedures

Use these procedures on this form.

Add a Holiday

1. Click [Add].
2. In the **Name** field, type a unique description or name for the holiday.
3. If you want this holiday to be of one or more types, indicate so by selecting the corresponding check box(es).
4. Select a start date on the calendar.
   - To select a month, click on the and navigation buttons. You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
   - Navigate to a year by clicking on the displayed year to access the year spin buttons, and then choose the year that you wish.
   - Once you have selected a month and a year, click on the day that you want the holiday to start on.
5. In the **Duration (days)** field, select the number of days that you want the selected holiday to last.
6. Click [OK]. The information will be updated in the listing window.

Modify a Holiday

1. In the listing window, select the name of the holiday you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Holiday

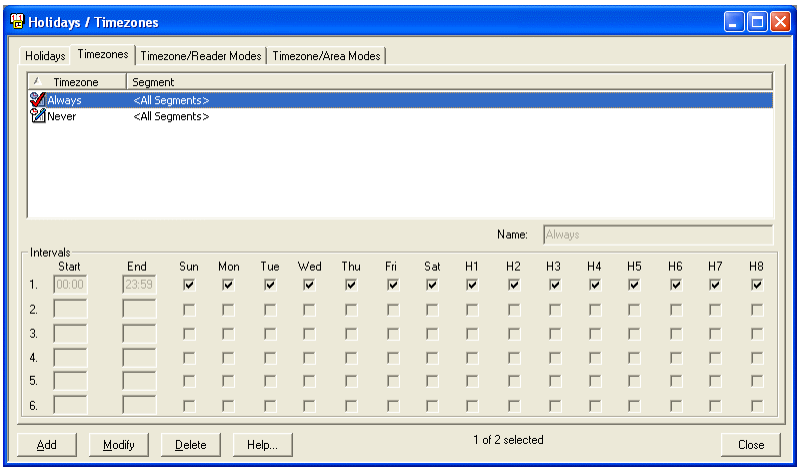
1. In the listing window, select the name of the holiday you wish to delete.
2. Click [Delete].
3. Click [OK].

Timezones Form

The Timezones form is used to create timezones, each consisting of up to 6 time range/day intervals. Selectable “days” include any of the seven days of the week, plus any of up to 8 holiday types (holiday types are defined on the Holidays form).

Hardware Dependencies: Lenel access panels support up to 255 timezones. All other access panels will accept a maximum of 127 timezones per panel. If your system contains both Lenel and non-Lenel access panels, you should consider using segmentation in order to avoid operator entry error and to take advantage of the extended performance features of the LNL-1000 access panel. If your system uses segmentation, your System Administrator determines the maximum number of timezones allowed per segment.

ILS access panels support five (5) time range/day intervals.



Timezone

Lists currently defined timezones.

ILS Integra

Only available to systems with ILS licenses. Select to indicate the timezone is to be downloaded to Integra systems. You can define up to 32 timezones as ILS Integra timezones including the two (2) system time intervals, Always and Never.

A ILS Integra timezone cannot be disabled if it is used by an Access Level or Timezone/Reader Modes entry containing Integra readers (locks). ILS Integra timezones must be associated with Integra readers (locks) in order to assign them to Access Level or Timezone/Reader Modes configurations.

ILS Offline/ILS Wireless

Only available to systems with ILS licenses. Select to indicate the timezone is to be downloaded to ILS offline or ILS wireless systems. You can define up to 64 timezones as ILS Offline/ILS Wireless timezones including the two (2) system time intervals, Always and Never.

An ILS Offline/ILS Wireless timezone cannot be disabled if it is used by an Access Level or Timezone/Reader Modes entry containing ILS readers (locks). ILS Offline/ILS Wireless timezones must be associated with ILS readers (locks) in order to assign them to Access Level or Timezone/Reader Modes configurations.

Name

Specifies the name of this timezone.

Intervals

Contains 6 lines (rows) of information, each of which includes **Start**, **End**, **Sun**, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, **H1**, **H2**, **H3**, **H4**, **H5**, **H6**, **H7**, and **H8** fields. Holiday types 3 - 8 are supported by Lenel access panels only. ILS access panels support five (5) intervals.

1

A particular timezone can be comprised of up to 6 time intervals, each of which is in effect on one or more days of the week (“days of the week” include Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, and holiday types 1 through 8). For the current timezone, complete the appropriate fields in this (first) row:

- The **Start** field represents the interval's starting time in military time. You can enter a value in the range of 00:00 through 24:00
- The **End** field represents the interval's ending time in military time. You can enter a value in the range of 00:00 through 24:00
- Click on **Sun** to put the Start-End interval in effect on Sundays
- Click on **Mon** to put the Start-End interval in effect on Mondays
- Click on **Tue** to put the Start-End interval in effect on Tuesdays
- Click on **Wed** to put the Start-End interval in effect on Wednesdays
- Click on **Thu** to put the Start-End interval in effect on Thursdays
- Click on **Fri** to put the Start-End interval in effect on Fridays
- Click on **Sat** to put the Start-End interval in effect on Saturdays
- Click on **H1** to put the Start-End interval in effect on Type 1 holidays. Do the same for any of the other defined holiday types (check boxes **H2** through **H8**) that you want to include in the timezone.

2

If the current timezone is to include two or more day/time intervals, complete the appropriate fields in rows 1 and 2.

3

If the current timezone is to include three or more day/time intervals, complete the appropriate fields in rows 1 through 3.

4
If the current timezone is to include four or more day/time intervals, complete the appropriate fields in rows 1 through 4.

5
If the current timezone is to include five or more day/time intervals, complete the appropriate fields in rows 1 through 5.

6
If the current timezone is to include six or more day/time intervals, complete the appropriate fields in all rows (1 through 6).

Add
Used to add a timezone entry.

Modify
Used to change a timezone entry.

Delete
Used to remove a timezone entry.

Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the Timezones folder.

Timezone Form Procedures

Use the following procedures on this form.

Add a Timezone

1. Click [Add].
2. Type a **Name** for the timezone.
3. Define each time interval in this Timezone, including the start and end times, the specific days of the week, and the holiday types that you want. Enter **Start** and **End** times, then select the check boxes that you want the time range to apply to.
4. A timezone can consist of up to 6 such intervals.
5. Click [OK].

Modify a Timezone

1. In the listing window, select the name of the timezone you wish to change.
2. Click [Modify].

3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Timezone

1. In the listing window, select the name of the timezone you wish to delete.
2. Click [Delete].
3. Click [OK].

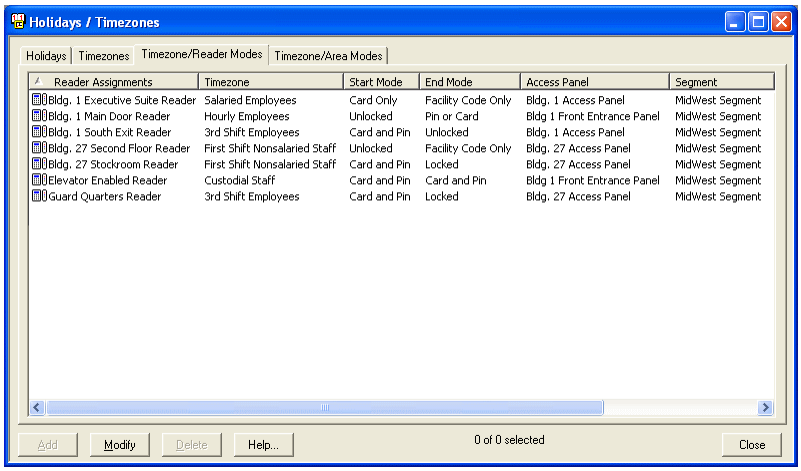
Timezone/Reader Modes Form

This form is used to:

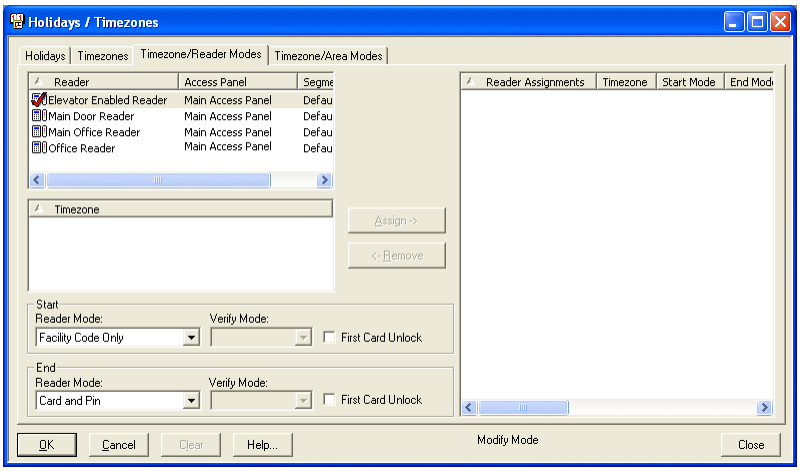
- For a given reader, choose individual operating modes for the beginning and the end of a particular timezone
- Remove the association between a particular timezone and a particular reader

Note: For readers connected to HID panels, the scheduled Unlocked mode is supported. To configure the scheduled Unlocked mode for an assigned timezone, select “Unlocked” for the (Start) **Reader Mode** and “Default” as the (End) **Reader Mode**. For more information, refer to the procedure Select Modes of Operation for a Reader During a Timezone on page 714.

Timezone/Reader Modes Form (View Mode)



Timezone/Reader Modes Form (Modify Mode)



Listing window

Lists currently defined readers. Each entry also indicates the **Timezone**, **Start Mode**, and **End Mode** assignments, plus the access panel to which the reader is attached and the segment involved (if segmentation is enabled).

Timezone

Selects a timezone to be associated with the selected reader.

Start

Contains the **Reader Mode**, **Verify Mode**, and **First Card Unlock** fields.

Reader Mode

Specifies the mode the reader will operate in at the beginning of the timezone.

For ILS offline/wireless readers (locks), the available modes include **Card Only**, **Facility Code Only**, **Unlocked**, and **First Card Unlock**. In **Facility Code Only** mode, the door is set to be opened by a card with a valid facility code, authorization level, and card activate/deactivate date.

For Integra readers (locks), the available modes include:

- **Card and Pin** - The door is set to be opened with a card and pin.
- **Card and Pin Unlocked** - Similar to the Card and Pin mode but the lock can be set to the Unlocked mode by entering the PIN and performing a double swipe of the card. A second double swipe of the card will revert the mode back to Card and Pin.
- **Card Only** - The door is set to be opened with a card only. Each user must use a valid card to open the door.
- **Cipher or Card** - Similar to the Card Only mode, allows the lock to be opened using the Lock PIN number, which should not be confused with the user pin.
- **Unlocked** - The door is unlocked.
- **First Card Unlock** - The first valid card that uses the lock unlocks the door. The lock is then placed in Unlocked mode.

Verify Mode

This field is used in conjunction with the **Biometric Verify** check box on the Readers form in the Readers folder. If that check box is selected, for alternate reader support, the primary reader will ask for verification from the alternate reader. Choose an option from this drop-down list to specify when the reader is to be in biometric verify mode.

First Card Unlock

Select this check box to enable the first card unlock feature for this timezone/reader mode. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., Card Only, Card and Pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will be required to present their card. After access is granted, the reader mode will change to Unlocked. This feature is useful for days like “snow days” when employees cannot make it to work on time. If the reader is in Facility Code Only mode, the first card unlock feature does not work.

End

Contains the **Reader Mode**, **Verify Mode**, and **First Card Unlock** fields.

Reader Mode

Specifies the mode the reader will operate in at the end of the timezone.

For ILS offline/wireless readers (locks), the available modes include **Card Only**, **Facility Code Only**, **Unlocked**, and **First Card Unlock**. In **Facility Code Only** mode, the door is set to be opened by a card with a valid facility code, authorization level, and card activate/deactivate date.

For Integra readers (locks), the available modes include:

- **Card and Pin** - The door is set to be opened with a card and pin.
- **Card and Pin Unlocked** - Similar to the Card and Pin mode but the lock can be set to the Unlocked mode by entering the PIN and performing a double swipe of the card. A second double swipe of the card will revert the mode back to Card and Pin.
- **Card Only** - The door is set to be opened with a card only. Each user must use a valid card to open the door.
- **Cipher or Card** - Similar to the Card Only mode, allows the lock to be opened using the Lock PIN number, which should not be confused with the user pin.
- **Unlocked** - The door is unlocked.
- **First Card Unlock** - The first valid card that uses the lock unlocks the door. The lock is then placed in Unlocked mode.

Verify Mode

This field is used in conjunction with the **Biometric Verify** check box on the Readers form in the Readers folder. If that check box is selected, for alternate reader support, the primary reader will ask for verification from the alternate reader. Choose an option from this drop-down list to specify when the reader is to be in biometric verify mode.

First Card Unlock

Select this check box to enable the first card unlock feature for this timezone/reader mode. If the reader is in Facility Code Only mode, the first card unlock feature does not work.

Assign

Associates the selected **Start mode** and **End mode** with this reader during the selected timezone.

Remove

Removes the association between the selected timezone and the selected reader modes.

Add

This button is not used. Use the [Assign] button to associate a timezone with a reader.

Modify

This button is used to change an existing timezone/reader assignment.

Delete

This button is not used. Use the [Remove] button to delete a reader-timezone association.

Help

Displays online assistance for this form.

Timezone/Reader Modes Form Procedures

Use the following procedures on this form.

Select Modes of Operation for a Reader During a Timezone

1. In the listing window, select the reader that you wish to control the operation of during a particular timezone.
2. Click [Modify].
3. Choose the **Timezone** you wish to configure for the selected reader.
4. In the Start section, from the **Reader Mode** drop-down, select the mode you want this reader to be placed in at the start of the selected timezone.
5. In the End section, from the **Reader Mode** drop-down, select the mode you want this reader to be placed in at the end of the selected timezone.
6. Click [Assign]. The following things happen immediately:
   - the change is saved to the database
   - the change is downloaded to the reader's access panel
   - the assignment window is updated

   Functionally, at the start of the selected timezone, the selected reader will begin to function in the selected **Start mode**. It will remain in that mode until the end of the timezone, at which time the reader will be placed in the selected **End mode**.
7. Repeat steps 3-6 for each additional timezone you wish to configure for this reader.
8. Click [OK] to return to view mode. The listing window will be updated to reflect your changes.
9. Repeat this procedure if you wish to select the operating modes of other readers.

Modify a Timezone/Reader Assignment

1. Click [Modify].
2. In the assignment window (located on the right side of the form), select the timezone/reader assignment you wish to change.
3. Make the changes you want for the **Timezone**, **Start mode**, and/or **End mode** selections.
4. Click [Assign] to immediately save the change to the database and download it to the access panel.
5. Repeat steps 1-4 for each other timezone/reader assignment you wish to change.
6. Click [OK] to return to view mode. The listing window will be updated to reflect your changes.

Remove a Timezone/Reader Assignment

1. Click [Modify].
2. In the assignment window (located on the right side of the form), select the timezone/reader assignment you wish to delete.
3. Click [Remove] to immediately save the change to the database and download it to the access panel.
4. Repeat steps 2 and 3 for each assignment to be removed.
5. Click [OK] to return to view mode. The listing window will be updated to reflect your changes.

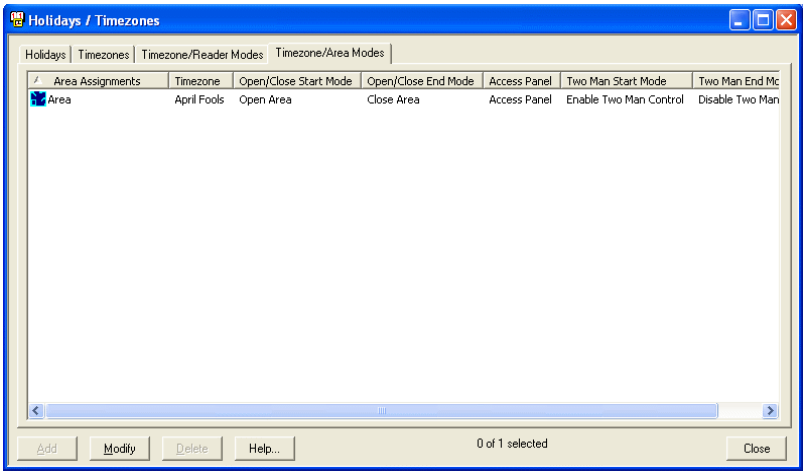
Timezone/Area Modes Form

This form is used to:

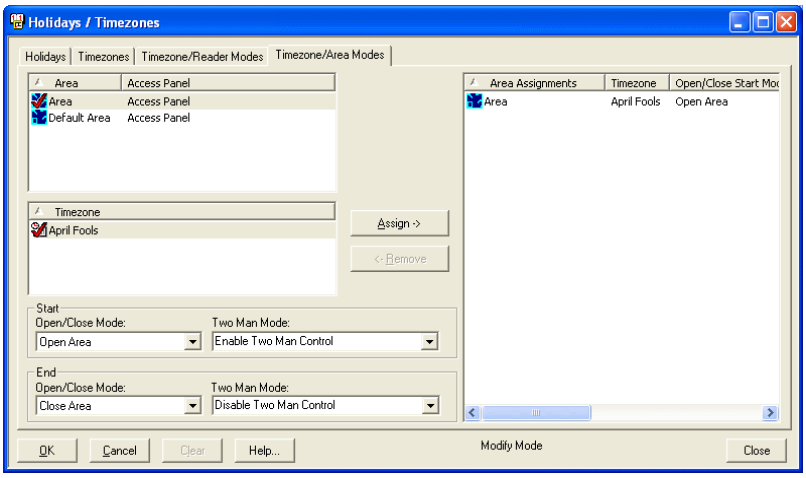
- For a given area, choose individual operating modes (including enabling or disabling Two Man Mode) for the beginning and the end of a particular timezone
- Remove the association between a particular timezone and a particular area

Note: The Open/Close Mode will be available to any local area on Lenel panels but the Two Man Mode will only be available to areas that belong to panels that have the special area rules enabled.

Timezone/Area Modes Form (View Mode)



Timezone/Area Modes Form (Modify Mode)



Listing window

Lists currently defined areas. Each entry also indicates the **Timezone**, **Open/Close Start Mode**, **Open/Close End Mode**, **Two Man Start Mode** and **Two Mad End Mode** assignments, plus the access panel to which the reader is attached and the segment involved (if segmentation is enabled).

Timezone

Selects a timezone to be associated with the selected area.

Start

Contains the **Open/Close Mode** and **Two Man Mode** fields.

Open/Close Mode

Allows you to change whether to open, close or have no change to the area access during the start of the specified timezone.

Two Man Mode

Allows you to change whether the Two Man Mode is enabled or not during the start of the specified timezone.

End

Contains the **Reader Mode**, **Verify Mode**, and **First Card Unlock** fields.

Open/Close Mode

Allows you to change whether to open, close or have no change to the area access during the end of the specified timezone.

Two Man Mode

Allows you to change whether the Two Man Mode is enabled or not during the end of the timezone.

Assign

Associates the selected **Start mode** and **End mode** with this area during the selected timezone.

Remove

Removes the association between the selected timezone and the selected area modes.

Add
This button is not used. Use the [Assign] button to associate a timezone with an area.

Modify
This button is used to change an existing timezone/reader assignment.

Delete
This button is not used. Use the [Remove] button to delete an area-timezone association.

Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the Timezones folder.

Start
Contains the **Open/Close Mode**, and **Two Man Mode** fields.

Timezone/Area Modes Form Procedures

Use the following procedures on this form.

Select Modes of Operation for an Area During a Timezone

1. In the listing window, select the area that you wish to control the operation of during a particular timezone.
2. Click [Modify].
3. Choose the **Timezone** you wish to configure for the selected reader.
4. In the Start section, from the **Open/Close Mode** drop-down list, select the mode you want this area to be placed in at the start of the selected timezone.
5. In the Start section, choose from the **Two Man Mode** drop-down list any changes you would like to make to the Two-Man Rule.
6. In the End section, from the **Open/Close Mode** drop-down list, select the mode you want this area to be placed in at the end of the selected timezone.
7. In the End section, choose from the **Two Man Mode** drop-down list any changes you would like to make to the Two-Man Rule.
8. Click [Assign]. The following things happen immediately:
   - the change is saved to the database
   - the change is downloaded to the reader’s access panel
   - the assignment window is updated

   Functionally, at the start of the selected timezone, the selected area will begin to function in the selected **Start mode**. It will remain in that mode until the end of the timezone, at which time the reader will be placed in the selected **End mode**.
9. Repeat steps 3-6 for each additional timezone you wish to configure for this area.

10. Click [OK] to return to view mode. The listing window will be updated to reflect your changes.
11. Repeat this procedure if you wish to select the operating modes of other area.

Modify a Timezone/Area Assignment

1. Click [Modify].
2. In the assignment window (located on the right side of the form), select the timezone/area assignment you wish to change.
3. Make the changes you want for the **Timezone**, **Start mode**, and/or **End mode** selections.
4. Click [Assign] to immediately save the change to the database and download it to the access panel.
5. Repeat steps 1-4 for each other timezone/area assignment you wish to change.
6. Click [OK] to return to view mode. The listing window will be updated to reflect your changes.

Remove a Timezone/Area Assignment

1. Click [Modify].
2. In the assignment window (located on the right side of the form), select the timezone/area assignment you wish to delete.
3. Click [Remove] to immediately save the change to the database and download it to the access panel.
4. Repeat steps 2 and 3 for each assignment to be removed.
5. Click [OK] to return to view mode. The listing window will be updated to reflect your changes.

CHAPTER 33

Access Levels Folder

The Access Levels folder contains forms with which you can:

- Define user access levels, each consisting of one or more reader/timezone combinations
- Define NGP intrusion levels, each consisting of one or more area/permission profiles.
- Define elevator access control types, and assign one or more elevator reader + timezone + elevator output/door combinations to each
- Group access levels into convenient access groups

The folder contains several forms: the Access Levels form, the Elevator Control form, and the Access Groups form. In addition, the Access Level Additional Segments form displays only if segmentation is enabled. The Extended Options form displays only if extended options are enabled in the system / segment.

The Precision Access form displays only if:

- The **Precision Access** check box is selected on the appropriate Access Panels folder.
- The Precision access mode is selected in the General Cardholder Options Form.
- At least one access level (not a precision access level) is assigned to the cardholder before a precision access level is assigned.

The Access Levels folder is displayed by selecting ***Access Levels*** from the ***Access Control*** menu, or by selecting the Access Levels toolbar button.

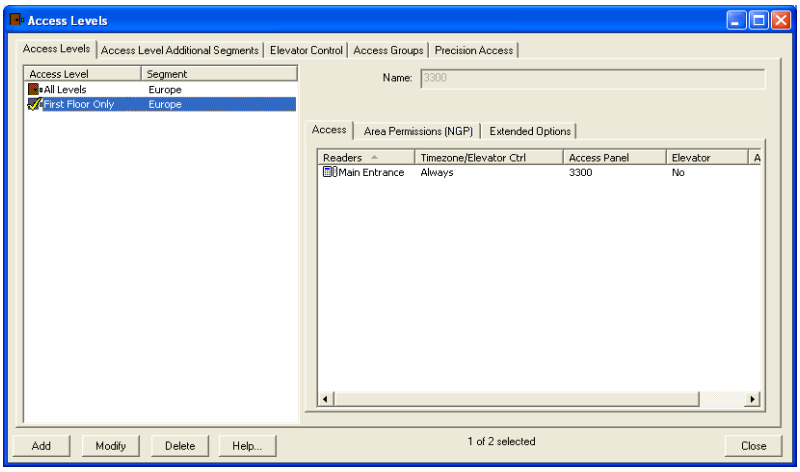
Toolbar Shortcut

Hardware Dependencies:

- The system supports connectivity to a variety of access panels. Each of the access panels provides different functionality and capabilities. One of the areas of varying functionality is access level support. The LNL-1000 can support up to 32,000 access levels.

- If your system contains LNL-1000 and non-LNL-1000 access panels, you should consider using segmentation in order to avoid operator entry error and to take advantage of the extended performance features of the LNL-1000 access panel.
- HID Edge panels support a maximum of eight (8) access levels per badge. If you add an access level that has an HID controller in common with 8 or more other access levels, some badges may exceed the limits of the controller, in which case only 8 access levels will be downloaded to this controller for those badges. Other HID controllers in the same access level may also be affected.
- Elevator dispatching systems do not support precision access levels.

Access Levels Form (Access Sub-tab - View Mode)



Note: What displays on this form differs depending on whether or not elevator dispatching support is enabled. The form differences are minor and are mainly seen in the menu headings for the listing windows. For more information, refer to the details in the table that follows.

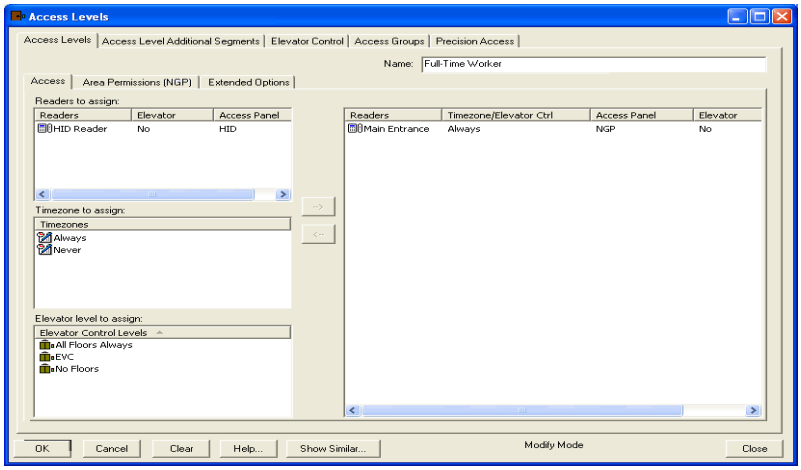
Listing window

(Displays in view mode only.) Lists currently defined access levels.

Access Levels Form (Access Sub-tab - Modify Mode)

The Access Levels form appears different when is used to:

- Define cardholder access levels.
- Assign one or more (reader + timezone) combinations to an access level.
- Assign one or more (elevator reader + elevator control level) combinations to an access level.
- Remove (reader + timezone) or (elevator reader + elevator control level) assignments.



Access Levels

(Displays in view mode only.) Lists currently defined access levels.

Name

Indicates the name of this access level

LCD name

The name as it will appear on the LCD reader display.

Assignment window

Each entry includes the following components:

- **Readers** - indicates the name of the reader
- **Timezone/Elevator Ctrl** - If the reader is an elevator reader, the elevator control level is indicated here. Otherwise, the name of the timezone is indicated. If no elevator is selected the Elevator Ctrl will be blank.
- **Access Panel** - indicates the name of the access panel to which the reader is connected
- **Elevator** - if Yes, the reader is an elevator reader. If No, the reader is not an elevator reader.
- **Area** - indicates the area the reader is assigned to.

Readers to assign

(displays in modify mode only) Each entry includes the following components:

- **Readers** - displays the name of the reader
- **Elevator** - displays name of the elevator to which the reader is associated or “No” if the reader is not associated with an elevator.
- **Access Panel** - displays the name of the access panel to which the reader is connected

Timezone to assign

(displays in modify mode only) Lists currently defined timezones

Elevator level to assign

(displays in modify mode only when an elevator reader is selected in the Readers to assign list) Lists currently defined elevator control levels.

Assign

Associates an access level with a reader and timezone

Remove
Removes the link between an access level to a reader and timezone.

Show Similar
Click to open the Similar Access Levels window. The Similar Access Levels window allows you to see access levels similar to the one you are trying to define. For more information, refer to Similar Access Levels Form on page 726.

Add
Adds an access level.

Modify
Changes an access level.

Delete
Removes an access level.

Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

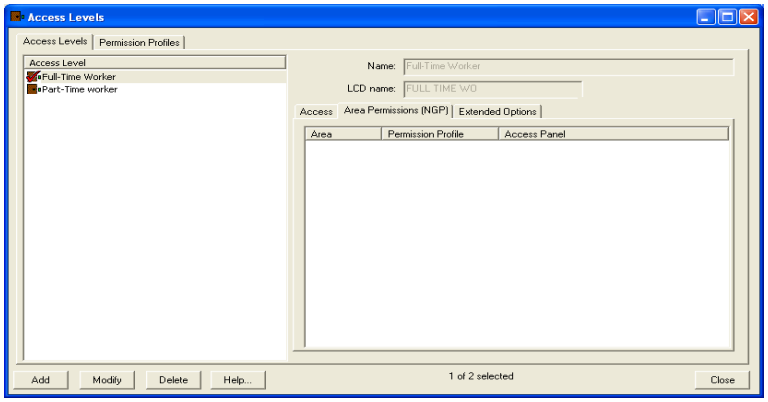
Close
Closes the Access Levels folder.

Access Levels Form (Area Permissions (NGP) Sub-tab)

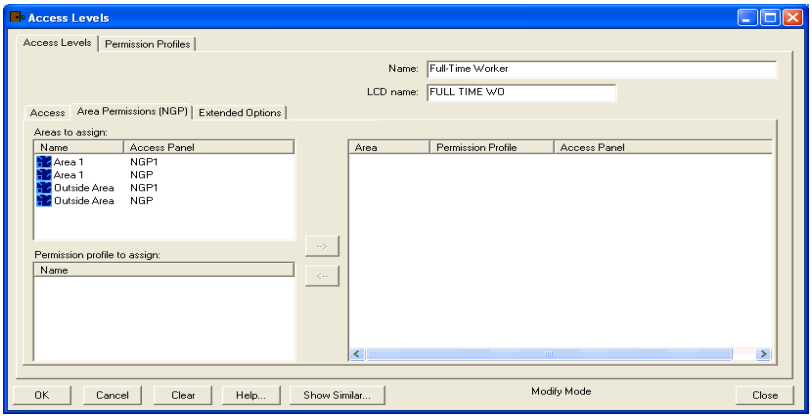
Note: This form is only available if an NGP panel is configured in the system

The Area Permissions (NGP) form is used to:

- Define cardholder intrusion access levels.
- Assign one or more (area + permission profile) combinations to an intrusion level.
- Remove (area + permission profile) assignments.



Access Levels Form (Area Permissions (NGP) Sub-tab Modify Mode)



Name

Indicates the name of this access level

LCD name

The name as it will appear on the LCD reader display.

Assignment window

Each entry includes the following components:

- **Area** - Indicates the area assigned to the intrusion level.
- **Permission Profile** - Indicates the permission profile assigned to the intrusion level.
- **Access Panel** - Indicates the access panel to which the intrusion level is assigned.

Areas to assign

(Displays in modify mode only) Each entry includes the following components:

- **Name** - Indicates the name of the area.
- **Access Panel** - Indicates the name of the access panel to which the area is assigned

Permission profile to assign

(Displays in modify mode only) Lists currently defined permission profiles.

Assign

Associates an intrusion level with a permission profile.

Remove

Removes the link between an intrusion level and a permission profile.

Show Similar

Click to open the Similar Access/Intrusion Levels window. The Similar Access/Intrusion Levels window allows you to see access/intrusion levels similar to the one you are trying to define. For more information, refer to Similar Access Levels Form on page 726.

Add

Adds an intrusion level.

Modify

Changes an intrusion level.

Delete
Removes an intrusion level.

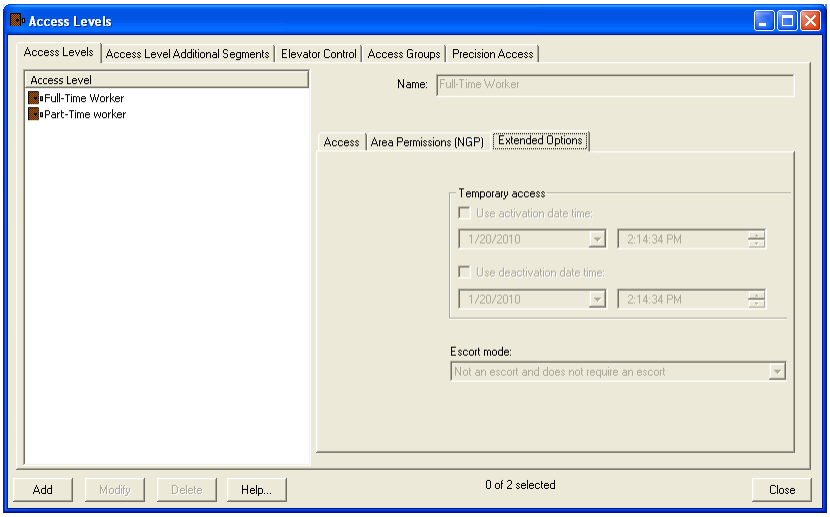
Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the folder.

Access Levels Form (Extended Options Sub-tab)

The form is used to configure temporary access to the access levels.



Listing window
Lists currently defined access levels.

Use activation date time
An access level can have an activation date and/or a deactivation date. Outside of these date ranges, the access level will have an effective time zone of “never”. The activation date can be set to “None” (disabled). Also, the granularity is to the second, so activation is based on time as well as a date. If enabled, activation date time is used in conjunction with the cardholder specific access level dates. Whichever has the latest activation date is used.

Use deactivation date time
An access level can have an activation date and/or a deactivation date. Outside of these date ranges, the access level will have an effective time zone of “never”. The deactivation date can be set to “None” (disabled). Also, the granularity is to the second, so activation is based on time as well as a date. If enabled, deactivation date time is used in conjunction with the cardholder specific access level dates. Whichever has the earliest deactivation date is used.

Escort mode

You can extend access level options to include escort access by selecting an escort mode. Choices include:

- Not an escort and does not require an escort
- An escort
- Requires an escort

A cardholder assigned to an access level that gives them escort access is allowed to escort cardholders who are assigned to an access level that requires an escort access.

Access Levels Form Procedures

Use the following procedures on this form.

Add an Access Level

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for this access level.
3. In the **LCD name** field, type the name as it will appear on the LCD reader display.
4. In the **Assign to Access Level** field, select one or more readers. If you have multiple readers selected simultaneously, they all must be the same type (either all elevator readers, or all non-elevator readers).

   To select a reader you must click on the icon to the left of it. A reader is selected if there is a checkmark on its icon, like this:
5. Do one of the following:
   - If the selected readers are elevator readers, select an entry in the **Elevator Control Levels** field
   - Select an entry in the **Timezones** field

   Although you can select multiple readers simultaneously, you can only select one Elevator Control Level or Timezone. An entry is selected if there is a checkmark on its icon.
6. Click [Assign]. An entry will be inserted into the assignment window for each selected reader.
7. Repeat steps 4-6 for each Elevator Control Level or Timezone you want to include in this access level.
8. To remove one or more reader assignments from this access level:
   a. In the assignment window, click on the entry or entries that you want to remove. [Remove] will become active.
   b. Click [Remove]. The entry or entries will be removed from the assignment window.
9. Click [OK]. The name of the access level will be inserted alphabetically into the Access Levels list. When you select the name, the readers that you assigned will be listed in the assignment window.
   - Each reader entry indicates that the reader can be used on specific days during specific time intervals.
   - Each elevator reader entry indicates that the elevator reader can be used to reach specific floors on specific days during specific time intervals.

   A cardholder having that access level would have the capabilities defined by all of the associated (reader + timezone/elevator control level) entries.

Assign Extended Options to an Access Level

You can assign escort access or require an escort access to access levels. A cardholder with escort access is allowed to escort cardholders who are not allowed in specific access levels.

1. From the ***Access Control*** menu, select ***Access Levels***. The Access Levels folder opens.
2. Click the Extended Options sub-tab.
3. Select (place a check mark beside) an access level.
4. Click [Modify].

Note: If the modify button is disabled, you need to enable extended options. This is done in the System Options folder for non-segmented systems or the Segments folder in segmented systems.

5. Select the escort mode from the drop-down list.
6. To configure an activation date/time, select the **Use activation date time** check box. Select the date and time using the drop-down list and spin buttons.
7. To configure the deactivation date/time, select the **Use deactivation date time** check box. Select the date and time using the drop-down list and spin buttons.
8. Click [OK].

Add an NGP Intrusion Level

For more information, refer to NGP Procedures on page 1568.

Modify an Access Level

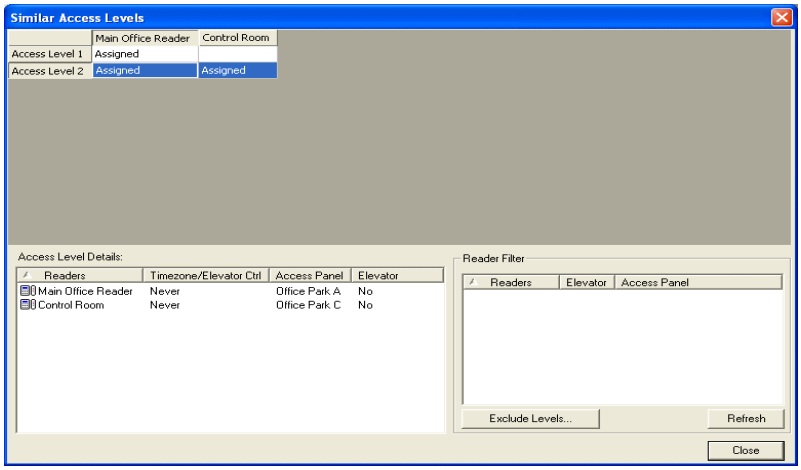
1. In the Access Levels window, select the name of the access level you wish to change.
2. Click [Modify].
3. Make the changes you want.
4. Click [OK] to save the change, or [Cancel] to revert to the previously saved assignments.

Delete an Access Level

1. In the Access Levels window, select the name of the access level you wish to delete.
2. Click [Delete].
3. Click [OK].

Similar Access Levels Form

While creating an access level, use the **Show Similar** button to see other access levels that have similar assignments to the one you are creating. Doing this helps stop the creation of duplicate access levels.



Reader filter

Select or deselect the reader to view or hide access levels that use that reader.

Areas filter

Select or deselect the area to view or hide access levels that use that reader.

Exclude Levels

Click to open the Exclude Levels window. The Exclude Levels window allows you to choose the access level to exclude when filtering similar access levels.

Refresh

After selecting a reader click this button to refresh the listing window.

Similar access levels

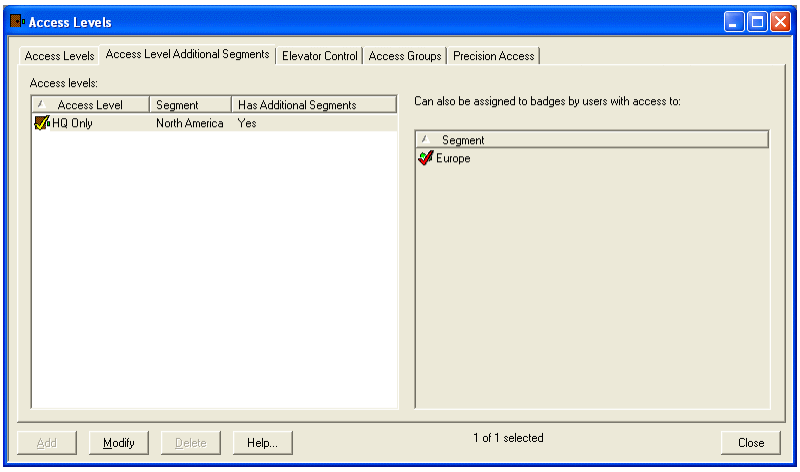
Shows the access levels similar to the one selected.

Close

Click to close the window.

Access Level Additional Segments Form

This form allows you to specify that a selected access level in one segment can also be assigned to badges by users with access to other selected segments.



Access levels listing window

Lists currently defined access levels, the segment each is associated with, and whether the access level has additional segments.

Segments listing window

In modify mode, all segments display. If a segment is selected, that access level can also be assigned to users with access to that segment.

In view mode, only selected segments display.

Modify

Changes the additional segments that an access level can be assigned to.

Help

Displays online assistance for this form.

Close

Closes the Access Levels folder.

Access Level Additional Segments Form Procedures

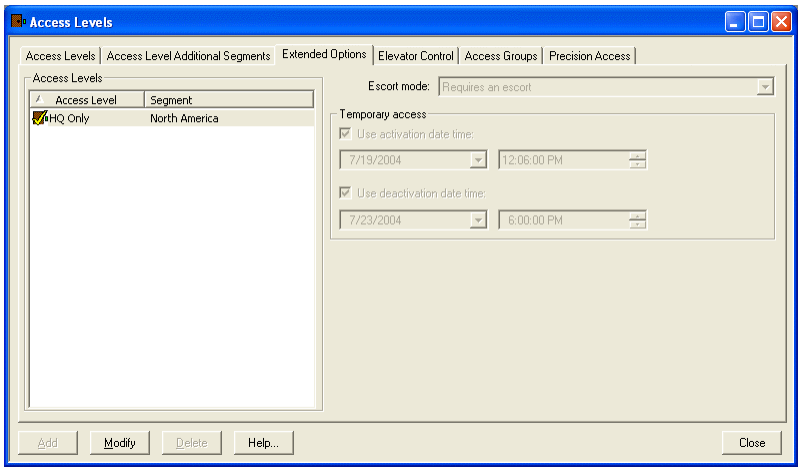
Use the following procedures on this form.

Modify an Access Level for Additional Segments

1. On the Access Level Additional Segments form in the Access levels listing window, select the access level you wish to make available to additional segments.
2. Click [Modify].
3. In the Segments listing window, select any additional segments you want the access level to be able to be assigned to.
4. Click [OK].

Extended Options Form

Note: Extended options are enabled (the Extend Options form is enabled) in the System Options folder for non-segmented systems or the Segments folder in segmented systems.



Access Levels

Lists currently defined access levels and the segment each is associated with.

Escort mode

You can extend access level options to include escort access by selecting an escort mode. Choices include:

- Not an escort and does not require an escort
- An escort
- Requires an escort

A cardholder assigned to an access level that gives them escort access is allowed to escort cardholders who are assigned to an access level that requires an escort access.

Use activation date time

An access level can have an activation date and/or a deactivation date. Outside of these date ranges, the access level will have an effective time zone of “never”. The activation date can be set to “None” (disabled). Also, the granularity is to the second, so activation is based on time as well as a date. If enabled, activation date time is used in conjunction with the cardholder specific access level dates. Whichever has the latest activation date is used.

Use deactivation date time

An access level can have an activation date and/or a deactivation date. Outside of these date ranges, the access level will have an effective time zone of “never”. The deactivation date can be set to “None” (disabled). Also, the granularity is to the second, so activation is based on time as well as a date. If enabled, deactivation date time is used in conjunction with the cardholder specific access level dates. Whichever has the earliest deactivation date is used.

Modify

Changes an access level option.

Help
Displays online assistance for this form.

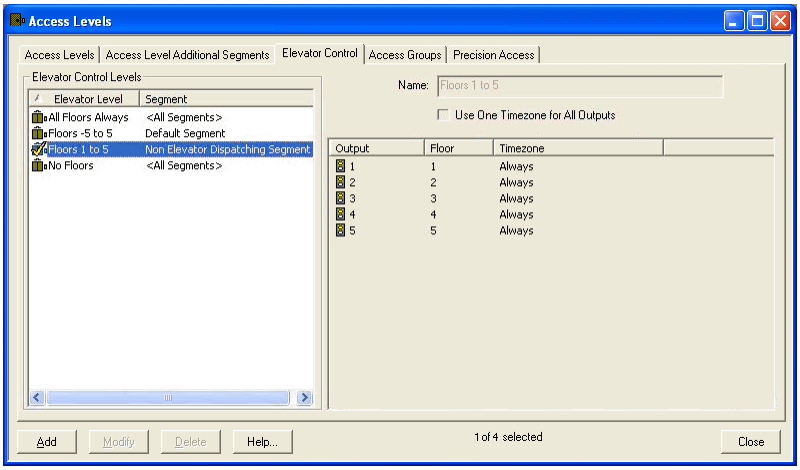
Close
Closes the Access Levels folder.

Elevator Control Form

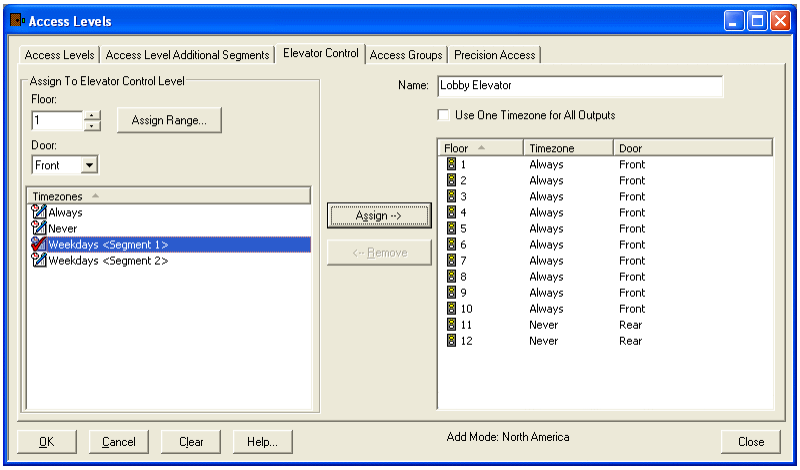
his form is used to:

- Define elevator control levels.
- Assign (reader output + timezone) combinations to an elevator control level.
- Remove (reader output + timezone) assignments.

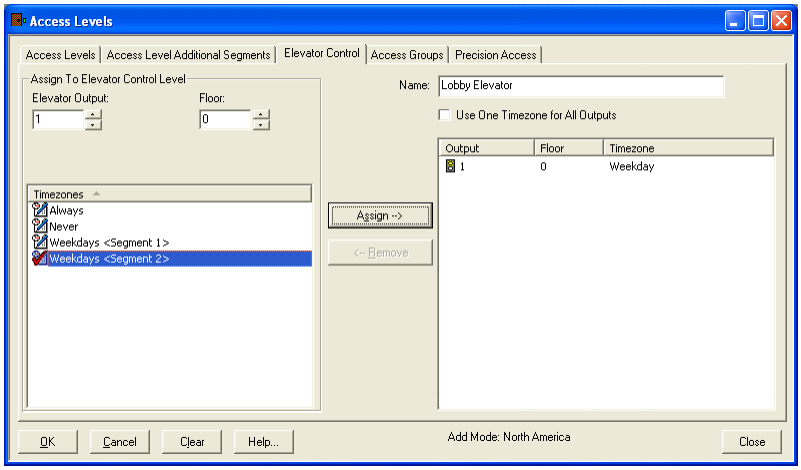
Elevator Control Form (View Mode)



Elevator Control Form (Modify Mode)



Note: This form looks different depending on whether or not elevator dispatching is enabled. The differences are minor and consist mostly of different column headings of the listing windows. They are detailed in the table below. If elevator dispatching is configured, use this form to assign (floor + timezone) combinations or remove such assignments.



Elevator Control Levels

(displays in view mode only) Lists currently defined elevator control levels and the segment each is associated with, if segmentation is enabled. (The Segment column will only appear if segmentation is enabled on your system.) An icon precedes each entry.

Name

Specifies a name for this elevator control level. Two types are pre-defined. They are:

- **All Floors Always** (all floors are always accessible)
- **No Floors**

You can create additional elevator control levels to fit your needs.

Use One Timezone for All Outputs

If selected, the currently selected timezone will be assigned to all (output) entries in the assignment window. Existing entries will be changed to reflect this. If not selected, you can assign a different timezone for each output. When elevator dispatching is configured, select **Use One Timezone for All Floors** to assign the timezone to all floor entries.

Assignment window

Each entry includes the following components:

- **Floor** - indicates the floor number associated with the output or the default floor for elevator dispatching configurations
- **Timezone** - indicates the name of the timezone
- **Door** - indicates which door is associated with the default floor for elevator dispatching configurations

Included only if elevator dispatching is not configured:

- **Output** - indicates the output number of the elevator reader

Assign To Elevator Control Level

(displays in modify mode only) Includes the **Floor**, **Timezones**, and **Door** fields. Includes the **Elevator Output**, **Floor**, and **Timezones** fields when elevator dispatching is not configured.

Elevator Output

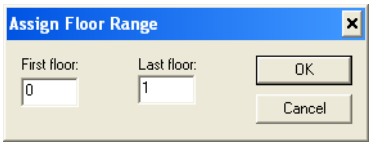
(displays in modify mode only when elevator dispatching is not configured) Indicates which output is lit on the elevator reader's output module. Possible values are in the range of 0 through 31.

Floor

(displays in modify mode only) When elevator dispatching is not configured, indicates the actual floor number associated with the output. This field is used for your reference. With elevator dispatching enabled, indicates the floor number(s) associated with the timezone.

Assign Range

(displays in modify mode only when elevator dispatching is configured) Opens a dialog allowing you to associate more than one floor with a timezone. Enter the **First floor** through the **Last floor** in the range, and then click [OK].



Door

(displays in modify mode only when elevator dispatching is configured) Indicates which door is associated with the floor.

Timezones

(displays in modify mode only) Select a timezone from those listed for this segment.

Assign -->

Associates an elevator control type with a reader output + timezone combination. For elevator dispatching configurations, associates an elevator control type with a floor + timezone combination.

<--Remove

Removes the link between an elevator control type and a reader output + timezone combination. For elevator dispatching configurations, removes the link between an elevator control type and a floor + timezone combination.

Add

Adds an elevator control entry.

Modify

Changes an elevator control entry.

Delete

Removes an elevator control entry.

Help

Displays online assistance for this form.

Close

Closes the Access Levels folder.

Elevator Control Form Procedures

An elevator control level consists of one or more (output/floor + timezone) combinations. Each such entry indicates that a particular floor can be accessed on specific days during specific time intervals.

A cardholder whose access level includes a particular elevator control level would have the capabilities defined by all of the associated (output/floor + timezone) entries.

Add an Elevator Control Level

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for this elevator control level.
3. In the **Elevator Output** field, use the spin buttons to select the number of the output to be activated. Or, you can highlight the value in the field, then type the output number.
4. In the **Floor** field, type the number of the floor that corresponds to this output. This step is not required; it is for your reference only. However, if elevator dispatching is configured, this step is required.

Note: If elevator dispatching is configured, in the **Door** field, select which door corresponds to the **Floor**.

5. In the **Timezones** field, select the name of a timezone.
6. If you want this timezone to apply to all outputs in this elevator control level, select the **Use One Timezone for All Outputs** check box.

Notes: If elevator dispatching is configured, select the **Use One Timezone for All Floors** check box if you want to apply this timezone to all floors in this elevator control level.

Selecting this check box will also affect any outputs (or floors) that have already been assigned to this elevator control level. In such instances, you will be asked whether you want to change the timezone for all output (floor) assignments.

7. Click [Assign].
8. For each output you want activated, repeat steps 3-5 and 7 (skip step 5 if you selected the **Use One Timezone for All Outputs** check box).
9. Click [OK].

Modify an Elevator Control Level

1. In the **Elevator Control Levels** field, select the name of the elevator control level you wish to change.
2. Click [Modify].
3. Make the changes you want.
4. Click [OK] to save your changes, or [Cancel] to revert to the previously saved values.

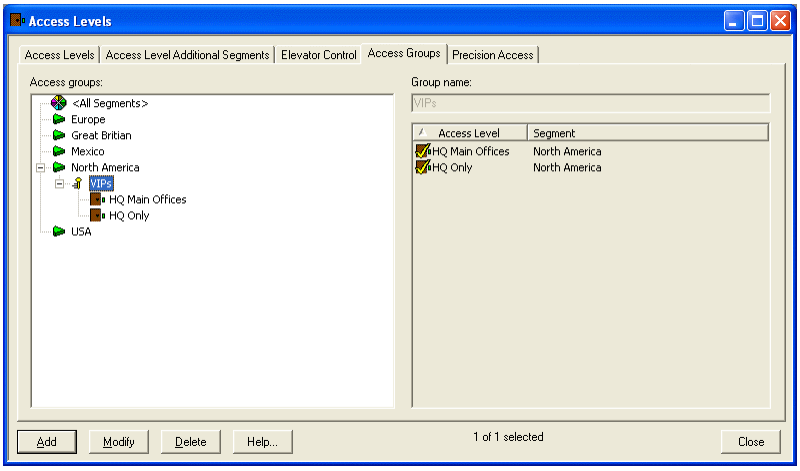
Delete an Elevator Control Level

1. In the **Elevator Control Levels** field, select the name of the elevator control level you wish to delete.
2. Click [Delete].
3. Click [OK].
4. You will be prompted with a reminder that deleting the elevator control level will affect elevator access for all badges linked to it. Click [Yes] to proceed with deletion.

Access Groups Form

This form is used to define access groups and to assign one or more access levels to a particular group.

Note: HID Edge supports a maximum of eight (8) access levels per badge. If you attempt to assign an access level to a group that would result in more than 8 access levels containing a common HID controller, it will not be assigned, and an error message will display listing the 8 access levels already assigned.



Access Groups

Lists currently defined access groups, and the access levels associated with each. If your system is segmented, the access groups will be shown in the segment they belong to. An icon precedes each access group entry. An icon precedes each access level entry.

Group Name

Indicates the name of this access group

Access Levels

Lists currently defined access levels and the segment each is associated with, if segmentation is enabled. (The Segment column will only appear if segmentation is enabled on your system.)

Add

Adds an access group entry.

Modify

Changes an access group entry.

Delete

Removes an access group entry.

Help

Displays online assistance for this form.

Close

Closes the Access Levels folder.

Access Groups Form Procedures

Use the following procedures on this form.

Add an Access Group

1. Click [Add].
2. In the **Group Name** field, type a unique, descriptive name for this access group.
3. Select the icon(s) that correspond to the access levels you wish to include in this group. Access levels are defined on the Access Levels form of this folder.
4. Click [OK]. The name will be added in alphabetical order to the Access Groups list.

Modify an Access Group

1. In the Access Groups list, select the name of the access group you wish to change.
2. Click [Modify].
3. Make the changes you want.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an Access Group

1. In the Access Groups list, select the name of the access group you wish to delete.
2. Click [Delete].
3. Click [OK].

Precision Access Form

This form is used to assign specific readers to specific inclusion groups.

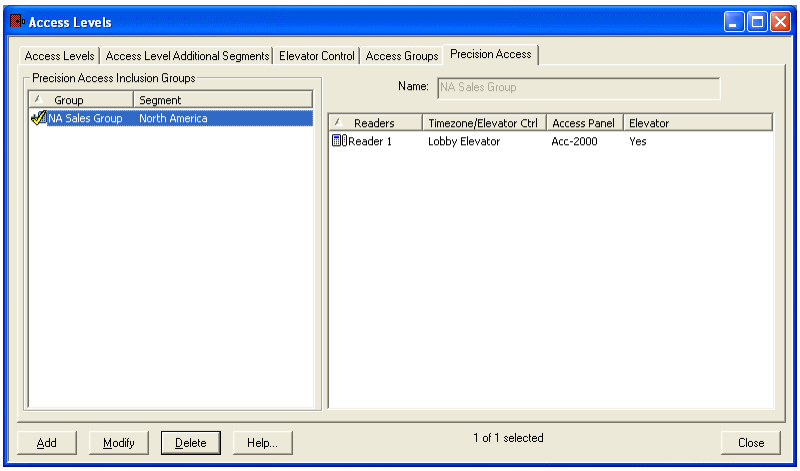
Most installations will not use the application's Precision Access capabilities. Those that do will have either inclusion or groups. *Inclusion groups* provide a way to select readers that someone CAN access during a specified timezone. These capabilities are used in addition to the normal access levels to further control access.

This form is displays only if "Inclusion" is selected in the **Precision Access Mode** field on the General Cardholder Options form in the Cardholder Options folder.

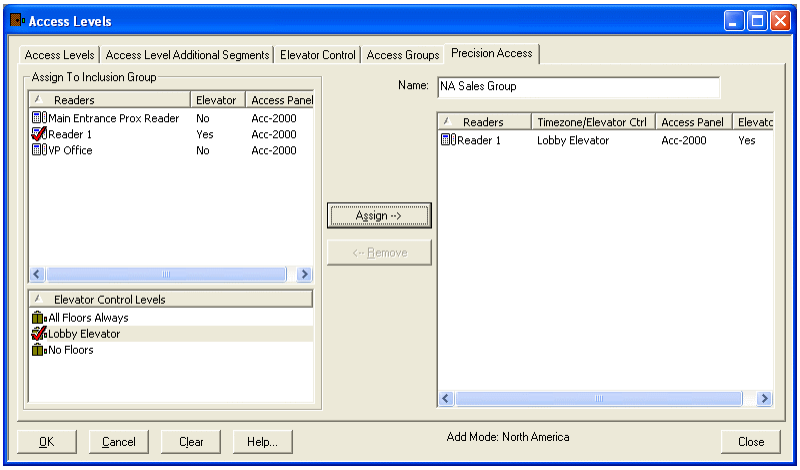
To configure precision access panel:

- Make sure the **Precision Access** check box is selected on the appropriate Access Panels folder.
- Select the Precision access mode in the General Cardholder Options Form.
- Assign at least one access level (not a precision access level) to the cardholder before a precision access level is assigned.

Precision Access Form (View Mode)



Precision Access Form (Modify Mode)



Precision Access Inclusion Groups

(displays in view mode only) Lists currently defined inclusion groups. An icon precedes each inclusion group entry.

Name

Indicates the name of the inclusion group

Assign to Inclusion Group

(displays in modify mode only) Each entry is preceded by an icon, and includes the following components:

- **Readers** - indicates the name of the reader
- **Elevator** - if Yes, the reader is an elevator reader. If No, the reader is not an elevator reader.
- **Access Panel** - indicates the name of the access panel to which the reader is connected

Timezones

(displays in modify mode only) Each entry is preceded by an icon. Select a timezone to be applied to the selected reader(s). Choices include all currently defined timezones.

Elevator Control Levels

(displays in modify mode only) Each entry is preceded by an icon. Select the elevator control level to be applied to the selected reader(s). Choices include all currently defined elevator control levels.

Assignment window

Each entry is preceded by an icon, and includes the following components:

- **Readers** - indicates the name of the reader
- **Timezone/Elevator Ctrl** - If the reader is an elevator reader, the elevator control level is indicated here. Otherwise, the name of the timezone is indicated.
- **Access Panel** - indicates the name of the access panel to which the reader is connected
- **Elevator** - if Yes, the reader is an elevator reader. If No, the reader is not an elevator reader

Assign

(displays in modify mode only) Adds one or more readers to a Precision Access inclusion group.

Remove

(displays in modify mode only) Removes one or more readers from a Precision Access inclusion group.

Add

Adds an inclusion group.

Modify

Changes an inclusion group.

Delete

Removes an inclusion group.

Help

Displays online assistance for this form.

Close

Closes the Access Levels folder.

Precision Access Form Procedures

Use the following procedures on this form.

Add a Precision Access Inclusion Group

1. From the ***Access Control*** menu, select ***Access Levels***. The Access Levels folder displays.
2. Click the Precision Access tab. If this tab does not available, refer to Precision Access Form on page 735.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this precision access inclusion group will be assigned to.

b. Click [OK].

5. In the **Name** field, type a unique, descriptive name for this group.
6. In the **Assign to Inclusion Group** field, select one or more readers to be contained in this group.
7. Do one of the following:
   - If the selected readers are elevator readers, select an entry in the **Elevator Control Levels** field.
   - If the selected readers are not elevator readers, select an entry in the **Timezones** field.

Note: Although you can select multiple readers simultaneously, you can only select one Elevator Control Level or Timezone. An entry is selected if there is a checkmark on its icon.

8. Click [Assign].
9. Repeat steps 6-7 for each different timezone to be included in the group. Note that a reader can be assigned to only one timezone. If you select a reader again and choose a different timezone, the change will be reflected in the assignment window.
10. Click [OK].

Modify a Precision Access Inclusion Group

1. In the Precision Access Inclusion Groups list, select the name of the group you wish to change.
2. Click [Modify].
3. Make the changes you want.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Precision Access Inclusion Group

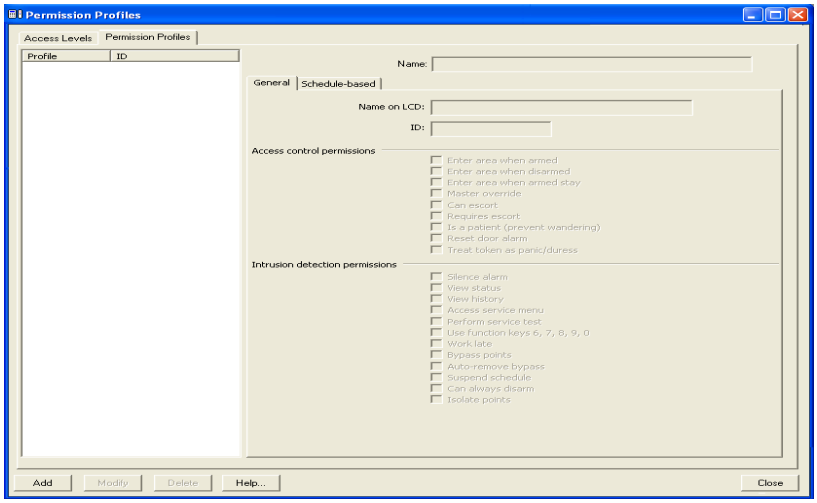
1. In the Precision Access Inclusion Groups list, select the name of the group you wish to delete.
2. Click [Delete].
3. Click [OK].

Permission Profiles (General Sub-tab)

The Permission Profiles form is used to define user permission profiles for the users of an NGP system. Permission profiles allow you to configure what parts of the system the users will be able to use and access.

IMPORTANT: To configure permission profiles you must have the correct permissions enabled. For more information, refer to System Permission Groups Form Procedures on page 362.

In an Enterprise system, you are unable to edit permission profiles at the master node when they are created at the child node.



Name

A name for the permission profile being created. This is a “friendly” name assigned to each permission profiles to make it easy to identify. Each name must be unique.

LCD Name

The name of the permission profile as it will appear on the LCD reader display.

ID

Enter the ID of the reader that will use these permissions.

Access Control Permissions

Permissions that control the access control areas of your system.

Enter area when armed

Select to allow users entrance to an area when it is armed.

Enter area when disarmed

Select to allow users entrance to an area when it is not armed.

Enter area when armed stay

Select to allow users entrance to an area when it is set to be armed stay.

Master override

Select to allow users to enter any door that would normally deny access.

Can escort

Select to assign a user to be an escort. A user who is assigned to be an escort helps guide visitors by using their credentials to pass through doors.

Requires escort

Select to allow a person to be tracked as they badge through doors. Their badge however will not open doors but instead must be opened using the credentials of an escort.

Is a patient (prevent wandering)

Select to prevent a patient from wandering and entering exterior doors or other areas of concern.

Reset door alarm
Select to allow the user to cancel a “Wandering Patient” alarm by presenting a token at the specific door.

Treat token as panic/duress
Select to treat a users token as a panic or duress alarm instead of an access request.

Intrusion Detection Permissions
Permissions that control the intrusion detection areas of your system.

Silence alarm
Select to allow users the ability to acknowledge an alarm at a panel.

View status
Select to allow a user the ability to view the status for the system and zones in the area.

View history
Select to allow a user to view the event history for the areas.

Access service menu
Select to access the service menu on the LCD keypad.

Perform system test
Select to allow users to perform a system test from an LCD keypad.

Use function keys 6,7,8,9,0
Select to allow users the ability to use programed hot keys.

Work late
Select to allow users the delay a closed schedule in 1/2 hour increments.

Bypass points
Select to allow users to set a bypass point on a panel to allow arming an area with a faulty sensor or broken window. A bypass remains in effect only until the area is disarmed.

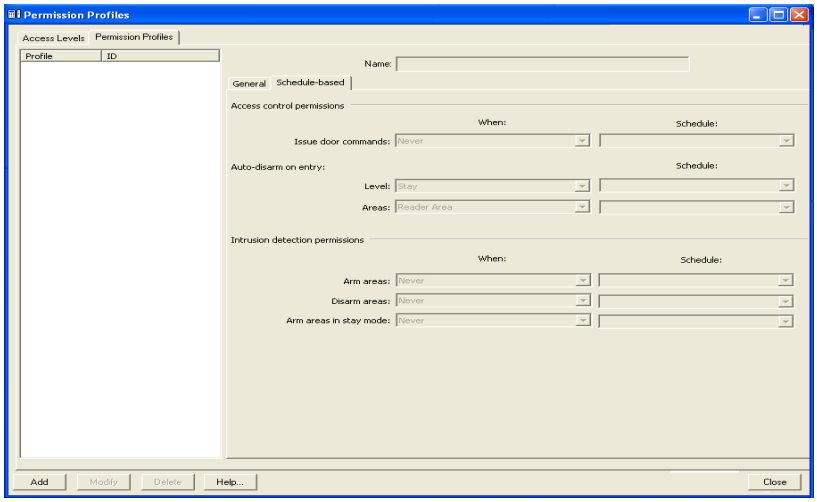
Auto-remove bypass
Select to automatically remove any bypass points that are in effect when an user is granted entry.

Suspend schedule
Select to allow users to suspend a schedule for an applicable area.

Can always disarm
Select to allow users to disarm an area.

Isolate points
Select to allow users to isolate input points or zones. Isolation remains in effect until it is manually removed.

Permission Profiles Form (Schedule-Based Sub-tab)



Access Control Permissions

This section's options allow you to configure access control options.

Issue Door Commands

Determines if and when associated users will be able to command doors in applicable areas through LCD-keypads or this software.

When

Used in conjunction with the **Issue Door Commands** field. Choices are:

- **Never** - select to never allow door commands to be issued.
- **Always** - select to always allow door commands to be issued.
- **In Schedule** - select to only allow door commands to be issued during the selected schedule.
- **Out of Schedule** - select to only allow door commands to be issued not during the selected schedule.

Schedule

Only applicable if the In Schedule or Out of Schedule options are selected at the When drop-down box. Select the schedule (the timezones configured in OnGuard) to be used for the permission profile.

Auto-Disarm On Entry

This section's options allow you to configure auto disarm options.

Level

Sets the arming-level (Off or Stay) for an 'Auto-Disarm' when a user associated with this authority gains entry to this area. Choices also allow having this depend on whether the event occurs during vs. outside of a chosen schedule.

Areas

Pertaining to an 'Auto-Disarm' (when a user associated with this authority gains entry to this area), this sets whether all areas in the authority will be disarmed, or only the one being entered. Choices also allow having this depend on whether the event occurs during vs. outside of a chosen schedule.

Schedule

Select the schedule (the timezones configured in OnGuard) to be used for the permission profile.

Intrusion Detection Permissions

This section's options allow you to configure intrusion detection options.

Arm Areas

Determines if and when associated users will be able to arm applicable areas (to ON). On: All sensors monitored (including interior motion detection).

Disarm Areas

Determines if and when associated users will be able to disarm applicable areas (to OFF). Off: Only 24-hour and life/safety sensors monitored.

Arm Areas in Stay Mode

Determines if and when associated users will be able to arm or disarm applicable areas (to STAY). Stay: Perimeter doors / sensors monitored (plus 24 hour/life-safety).

When

Choices Include Never, Always, In Schedule, Out of Schedule.

Schedule

Only applicable if the In Schedule or Out of Schedule options are selected. The combo box should include timezones configured in OnGuard.

CHAPTER 34

Command Keypad Templates Folder

The Command Keypad Templates folder allows you to create macros for key sequences that can be assigned to a function key of a command keypad, allowing cardholders the ability to use the reader's keypad to issue commands. These commands can have a multitude of functions including arming/disarming an area and contacting emergency personnel. You can also define display strings that appear on the reader's display screen and assign intrusion command authority.

To accomplish this you will create macros, assign them to specific function keys for a template, configure the display strings and intrusion command for a template, and then assign that template to a specific reader. The intrusion commands assigned to the template can only be executed from the reader by cardholders who have specific access level authority.

The Command Keypad Templates folder is used to:

- Assign macros to shorten keypad sequences into single or double digit inputs
- Assign which cardholder authority has access to certain commands
- Assign text that is displayed on the reader

Command Keypad Templates User Permissions

The Command Keypad Templates form needs to have certain user permissions enabled to work fully.

To assign permissions to use command keypad templates navigate to Administration > Users > System Permission Groups tab > Access Control sub-tab. Use the **Command keypad templates** check boxes to enable the features. To do this:

1. Select a user in the Permission Group listing window
2. Click [Modify]
3. Select the Command keypad templates check box and its corresponding add, modify, and delete check boxes.

Intrusion Authority Levels User Permissions

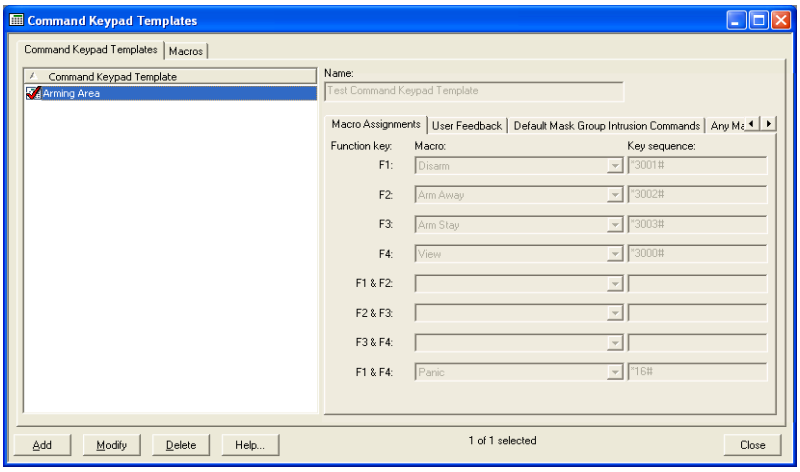
Once a command keypad template is created you will want to assign certain authority restrictions so only select cardholders can access the command keypad functions. You need proper cardholder permissions to do this.

To assign cardholders permission to use the command keypad templates navigate to Administration > Users > Cardholder Permission Groups tab > Badge sub-tab. Use the **Access level assignments** check boxes to enable the feature. To do this:

1. Select a user in the Permission Group listing window
2. Click [Modify]
3. Select the **Modify intrusion authority** check box. The selected users can now assign authority levels to cardholders.

Command Keypad Templates Form (Macro Assignments Sub-tab)

The Macro Assignments form is used to assign macros that you have created to the function keys of the keypad. The form is displayed by clicking ***Access Control > Command Keypad Templates***. For more information, refer to Key Sequence Format on page 748.



Command Keypad Template listing window

Lists any created templates.

Name

A user-defined name for a template. This should be a descriptive name.

Function key

Keys that correspond with the function keys on the command keypad. You assign macros to these keys.

Macro

Choose a macro that has been created to use with the corresponding function key.

Key sequence

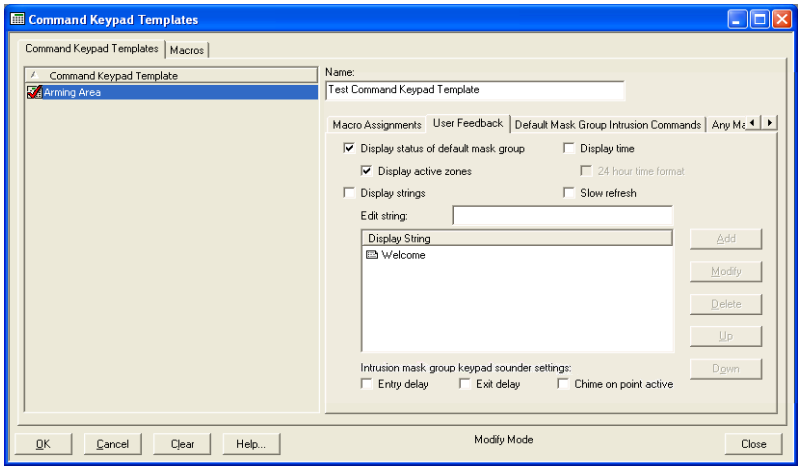
A listing of the key sequence used with the selected macro.

Command Keypad Templates Form (User Feedback Sub-tab)

The User Feedback sub-tab allows you to add pre-configured or custom made strings that are then displayed on your command keypad.

The form is displayed by selecting the menu option ***Access Control > Command Keypad Templates*** and then clicking User Feedback sub-tab. For more information, refer to Add/Edit Display Strings on page 750.

Note: The display strings are listed for the template in the same order in which they are displayed on the command keypad.



Display status of default mask group

Select to show the status of the default mask group on the command keypad.

Display active zones

Select to display the current active zones that are in a fault state and belong to the mask group.

Display time

Select to display the current time on the command keypad.

24 hour time format

After selecting the Display time check box, select this to display the time in the 24-hour format.

Display strings

Select to display the user created strings on the command keypad. For more information, refer to Add/Edit Display Strings on page 750.

Slow refresh

Check to slow the speed of the scrolling text on the LNL-CK display.

Edit string

Text box used to add or edit a display string. A display string can be a maximum of 16 characters.

Entry delay
Select to have the keypad produce an audio signal during an entry delay.

Exit delay
Select to have the keypad produce an audio signal during an exit delay.

Chime on point active
Select to have the keypad produce an audio signal when a point becomes active.

Add
Click to add a string to the command keypad display. The button will only become enabled once a string listed in the "Edit string" text box has been added or changed. Note that at most 8 display strings are allowed per template.

Modify
Click to Modify the string currently listed in the "Edit string" text box. This button will only become enabled once the string listed in the "Edit string" text box has changed.

Up
Select a display string and click [Up] to move it up in the queue.

Down
Select a display string and click [Down] to move it down in the queue.

Delete
Select a display string and click [Delete] to delete the string from the queue.

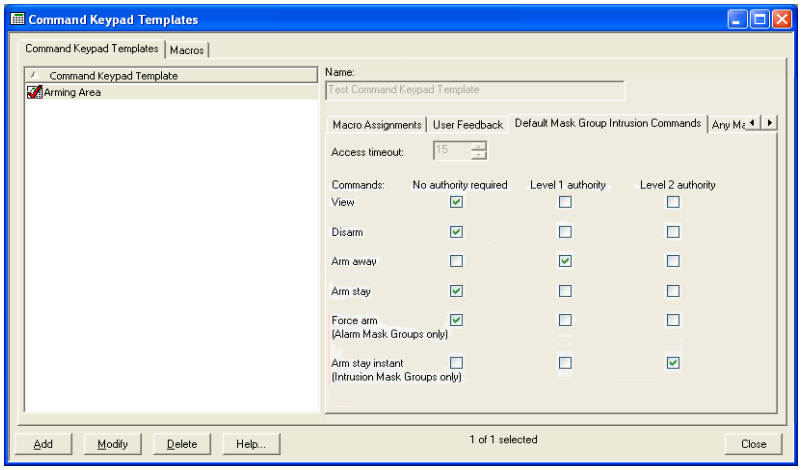
Command Keypad Templates Form (Default/Any Mask Group Intrusion Commands Sub-tab)

IMPORTANT: To use this feature you must first enable intrusion command configuration. Do this by selecting ***Administration > System Options*** > and clicking User Commands sub-tab. Then select "Advanced Permission Control" from the **Intrusion command configuration** drop-down. If you have segmentation enabled this option will be in the Segments folder. For more information, refer to User Commands Form on page 404.

The Default Mask Group Intrusion Commands sub-tab and the Any Mask Group Intrusion Commands sub-tab have the same user interface and function in a similar manner. They are both used to determine the authority permissions that are required to view, arm, disarm, and force arm, areas through the keypad.

The only difference between them is that the Default Mask Group Intrusion Commands sub-tab affects only the default mask group assigned to a reader. The Any Mask Group Intrusion Commands sub-tab determines authority permissions that are used for any mask group defined for a given controller.

The forms are displayed by selecting the menu option ***Access Control > Command Keypad Templates*** and then clicking Default Mask Group Intrusion Commands sub-tab or Any Mask Group Intrusion Commands sub-tab.



Access timeout

The amount of time (in seconds) that the user has to enter the command after presenting their badge.

Commands

The list of commands that you can assign authority to. Each command is associated with a number. This number is important to know when entering the key sequence into a macro or into the keypad itself as it is the command number that is entered at the reader to execute the specific command.

No authority

Check this box (next to the corresponding command) to make it so no authority is needed to use the command. Take care when assigning No authority to a command. This will make it so any cardholder can run this command.

Level 1 authority

Check this box (next to the corresponding command) to make it so that only cardholders with level 1 authority can use the command. To give a cardholder authority, go to the Cardholders folder and, after selecting a cardholder, navigate to the Access Levels sub-tab. Click [Intrusion Authority] and assign the appropriate authority.

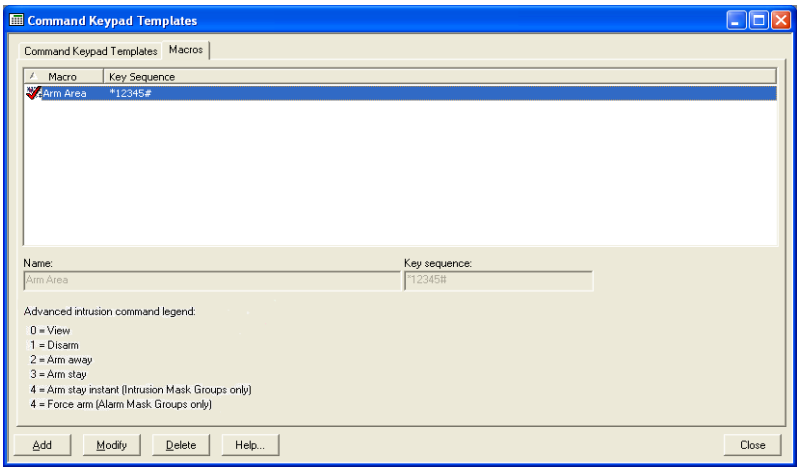
Level 2 authority

Check this box (next to the corresponding command) to make it so that only cardholders with level 2 authority can use the command. To give a cardholder authority, go to the Cardholders folder and, after selecting a cardholder, navigate to the Access Levels sub-tab. Click [Intrusion Authority] and assign the appropriate authority.

Macros Form

The Macros form is used to define macros to a keypad sequences in order to shorten the input to one or two keys. For example, instead of entering “*3000123” at the command keypad, a macro can be defined for this key sequence and assigned to one of the function keys.

The form is displayed by selecting the menu option ***Access Control > Command Keypad Templates*** and then clicking Macros. For more information, refer to Add a Macro on page 749.



Listing window

Lists the macro and the key sequence associated with it.

Name

Name of the macro you are creating.

Key sequence

Input the key sequence here that you wish to associate with the macro.

Key Sequence Format

The following key sequence formats are entered at the command keypad after the cardholder presents their badge.

Permission Control Format

The following key sequence format can be used when either “Global Permission Control Only” or “Advanced Permission Control” intrusion command have been chosen. For more information, refer to User Commands Form on page 404.

Note: The reader must be configured with the “Allow Intrusion Commands” option in order to accept this key sequence. For more information, refer to General Form on page 635.

*{command code}{2-digit mask group number}#

A menu is then displayed on the command keypad with various commands to be executed.

Default Mask Group Intrusion Command Format:

The following key sequence format only apply when the “Advanced Permission Control” intrusion command configuration is configured. For more information, refer to User Commands Form on page 404.

*{command code}{command number}#

This key sequence deals with the mask group assigned to the reader on the command programming tab of the Readers form. For more information, refer to Command Programming Form on page 669.

Any Mask Group Intrusion Command Format:

The following key sequence format only apply when the “Advanced Permission Control” intrusion command configuration is configured. For more information, refer to User Commands Form on page 404.

*{command code}{2-digit mask group number}{command number}#

The command numbers are as follows:

0 = View

1 = Disarm

2 = Arm away

3 = Arm stay (Intrusion Mask Groups only)

4 = Arm stay instant (Intrusion Mask Groups only)

4 = Force Arm (Alarm Mask Groups only)

Configuring the Command Keypad

The following procedures guide you through setting up a command keypad template with macros, display strings, and intrusion commands and then assigning that template to a reader.

In addition, the procedures will also guide you in how to assign authority to a cardholder in order for them to execute intrusion commands at the keypad based on the authority defined.

Setting up a Command Keypad Template and Associating with a Reader

Use the following procedures to set up a command keypad template and associate it with a reader.

Add a Macro

Note: A macro assignment is not required for a command keypad template.

1. Navigate to ***Access Control*** > ***Command Keypad Templates***. On the Macros form, click [Add].
2. Input a name for the macro.
3. In the Key sequence section add the key sequence that is to be associated with the macro. This usually includes a “*”, a 3-6 digit intrusion command code, a command, and “#”. For more information, refer to Key Sequence Format on page 748.
4. Click [OK].

Create a Command Keypad Template

1. Navigate to ***Access Control*** > ***Command Keypad Templates***. Click [Add].
2. Input a name for the template.
3. If you wish to add a Macro follow these steps:
   a. Click the Macros tab.
   b. Click [Add]
   c. Enter a name for the macro in the **Name** field.

d. Enter the key sequence you wish the macro to utilize in the **Key sequence** field.

e. Click [OK].

4. Choose a function key to correspond with any macros you created. On that function key's drop-down, select the macro to use. For more information, refer to Add a Macro on page 749.
5. On the Default or Any Mask Group Intrusion Commands form, check the appropriate commands that you wish the template to have. These commands mark what access authority the cardholder must have to run the commands from the keypad.
6. If you wish, you may change the default **Access timeout** to allow a longer or shorter period of time a cardholder has to execute intrusion commands after gaining access to the reader.
7. Click [OK].

Add/Edit Display Strings

The display strings are messages that you can have displayed at the command keypad. You may use these to instruct the cardholder what function key does what according to the macro that you made in the previous steps.

1. Navigate to ***Access Control*** > ***Command Keypad Templates***. Click the User Feedback sub-tab.
2. Select a Command Keypad Template from the listing box. Click, [Modify].
3. Enter a string into the "Edit string" text box and click, [Add]. You can also select an existing display string from the list, make changes to it in the "Edit string" text box and click, [Modify].
4. Select any of the pre-configured display string check-box options that you wish to add.
5. Click [OK].

Assign the Template to a Reader

With the template created you must now assign it to a reader on the Command Programming sub-tab of the Readers form. For more information, refer to Command Programming Form on page 669.

1. From the Access Control menu select Readers.
2. Select a compatible reader and click the Command Programming sub-tab.

Note: Compatible readers are those defined in a system/segment that is configured for the Advanced Permission Control intrusion command configuration. Also note that any reader with a keypad interface can utilize the Intrusion Command portion of the template. If the reader is a command keypad, it can also utilize the macro assignments and display string portion of the template.

3. Click [Modify].
4. In the **Command keypad template** drop-down, select the template that you created. You can also define the default mask group by selecting an option from the **Default mask group** drop-down box. For more information, refer to Command Programming Form on page 669.
5. Click [OK].

Assign Authority Access Levels to Cardholders

When you created the template you selected whether a cardholder will need a special authority access level to run commands from the keypad. To assign these authority access levels to a cardholder do the following:

1. Enable Intrusion command configuration. To do this:

a. Navigate to ***Administration*** > ***System Options***. On the User Commands tab, click [Modify].

b. On the **Intrusion command configuration** drop-down, select **Advanced Permission Control**. This will allow authority levels to be assigned to cardholders.

c. Make note of the **Intrusion command code** field. This code is important to issuing commands from the keypad and creating the macros.

d. Click [OK].

2. Navigate to ***Administration > Cardholders***. On the Cardholder screen, navigate to the cardholder you wish to give access to.
3. Click the Access Levels sub-tab. For more information, refer to Access Levels Form on page 117.
4. Click [Modify].
5. Click [Intrusion Authority]. A list of access levels that are configured in a system/segment are shown. Select what access levels for the selected cardholder you would like to assign Level 1 and/or Level 2 authority. You must have the proper permissions to do this. For more information, refer to Intrusion Authority Levels User Permissions on page 744.
6. Click [OK].

IMPORTANT: The authority levels assigned act as access levels but do not count toward the maximum number of access level assignment allowed per badge. When the “Advanced Permission Control” intrusion command configuration option is selected, the maximum number of access level assignments allowed per badge is reduced to 126.

CHAPTER 35

Areas Folder

The Areas folder contains forms with which you can:

- Create one or more named areas associated with a specific access panel. On the Anti-Passback form of the Readers folder, you can indicate which readers are used to enter a particular area
- If the panel supports it, specify anti-passback rules governing access to and occupancy of the area
- Define open areas with no area rules in effect, closed areas that allow access, and closed areas that allow limited or no access
- Create interlocking doors so that only one door to a specified area may be open at a time
- Link a local I/O function list to area occupancy levels
- Define associated safe locations
- Define associated inside areas
- Configure muster reporting
- Configure the Special Two Man rule

The folder can contain up to five forms, the Areas form, and if global anti-passback is enabled on your system, the Associated Safe Locations form, the Associated Inside Areas form, and the Muster Reporting form. If the Special Two Man Rule is enabled you will see the Special Two Man form.

The Areas Folder is displayed by selecting ***Areas*** from the ***Access Control*** menu, or by selecting the Areas toolbar button.

Toolbar Shortcut

Mustering Overview

In the event of an emergency incident, mustering can be used to gather cardholders together in a specified area. When an emergency incident occurs in a hazardous location, the system goes into muster mode. A Hazardous Location is a defined area that can have multiple entry and exit card readers. When the system is in muster mode, mustering out of a hazardous location area and into a

safe location area is required. A Safe Location is a defined area with muster readers that are configured to be used in the event of an emergency incident. A muster reader is a card reader that is used to define a hazardous location and can be designated as either an entry reader or an exit reader.

When an emergency incident occurs in a hazardous location, a muster report is generated. This report lists all of the cardholders that are currently in the hazardous location. Cardholders can register in a safe location by checking in at a specified muster reader. Once a cardholder has registered in a safe location, they are removed from the muster report. The muster report then becomes a report of all of the cardholders who were in the hazardous location at the time of the emergency incident, but who have failed to register at a safe location.

When safe locations are located outside of a hazardous location, when an incident occurs, cardholders have free access to leave the hazardous location. They are then required to register at a safe location outside of the hazardous location. When safe locations are located inside of a hazardous location, when an incident occurs, cardholders are not allowed to leave and must register at a safe location inside of the hazardous location.

IMPORTANT: For the purpose of tracking hazardous location and safe location occupancy, global APB must be enabled on your system in order to configure mustering.

To enable global APB:

- In a segmented system, select the **Global Anti-Passback** check box on the Anti-Passback sub-tab of the Segments form in the Segments folder.
- In a non-segmented system, select the **Global Anti-Passback** check box on the Anti-Passback form of the System Options folder.

Interlock Overview

In a situation where a controlled area is needed, readers in the area can be interlocked. This can be configured using areas. In an interlocked area, only one door may be opened at a time. For any door in the area, if the door strike is active or the door is open, no other door may be opened to leave or enter the area. Any additional request for access will be denied when the interlock is in this busy state.

If this is the case, an event will indicate it in Alarm Monitoring, and the LED on the other door reader(s) will show that it has been disabled.

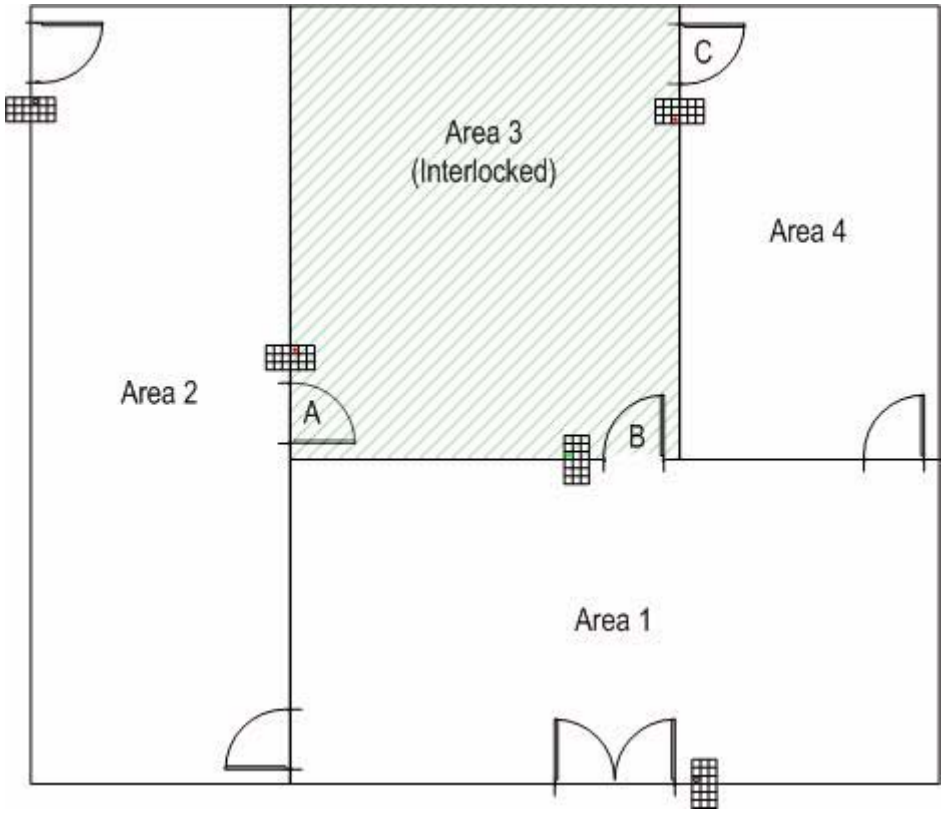
Interlock Area Busy. This occurs when access requested by presenting a valid credential was denied because a door is open or the door strike is active within an interlocked area.

Cannot Open Door: Interlock Area Busy. This occurs when an attempt to open the door in Alarm Monitoring was denied because a door is open or the door strike is active within an interlocked area.

Exit Request Denied: Interlock Area Busy. This occurs when a request to exit made via REX button was denied because a door is open or the door strike is active within an interlocked area.

DURESS - Interlock Area Busy. This occurs when access was requested to an interlocked area while under duress.

In the following diagram, Area 3 is an interlocked area. Since door B is open, or the door strike is active, the readers at doors A and C will not allow access.



This option is available for the LNL-2220 and LNL-3300 panels. This function can only be enabled for local anti-passback. If global anti-passback is enabled, this option will be unavailable.

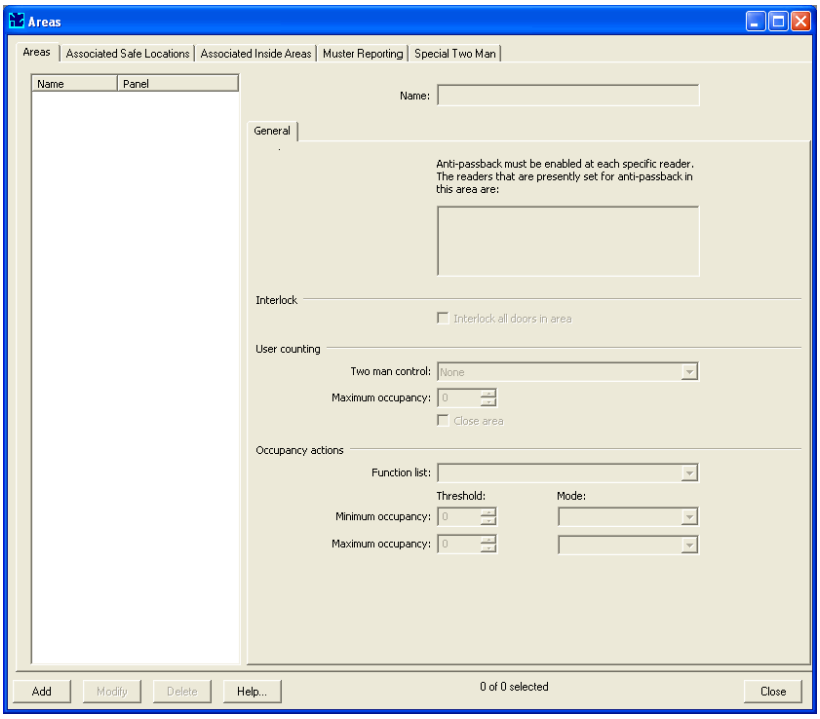
For more information on interlock configuration, refer to Configure an Interlocked Area on page 768.

Escorts and Turnstiles

If the system is configured for escorts, all members of the escorted group and the escort are to present their credentials. The interlock will only be considered busy once the escort's access request has been granted. This ensures that the interlock is not busy for longer than necessary. If the access request is denied because the interlock is busy, then everyone in the escorted group and the escort must present their credentials to the reader again to request access.

If the system is also configured for turnstiles in addition to escorts, once the access request has been granted, the interlock will be considered busy until everyone in the group has passed through the turnstile.

Areas Form (General Sub-tab)



Note: This screen appears differently depending on the panel you are using and whether you are using a local or global anti-passback areas.

Listing window

Lists currently defined areas and the access panel/segment associated with each.

Name

Specify a name for this area. You can enter a name containing a maximum of 32 characters.

Panel

This field does not appear when using global anti-passback. Select the access panel with which the area is associated. Choices include all currently defined access panels.

Name on LCD

This field is only available for NGP panels. The name as it will appear on the LCD reader display.

ID

This field is only available for NGP panels. Enter the ID as displayed on your NGP hardware. The ID acts as a unique identifier for the hardware.

Require function key PIN

This field is only available for NGP panels. Whether or not the programmable hot-keys 6-9 & 0 will require a user with “Function Key” authority to be logged in. (Function keys 1-5 do not require ID/PIN entry, except at a portable/wireless arming keypad).

Anti-Passback

This section allows you to configure anti-passback options.

Strict entry/exit enforcement

This field is only available for NGP panels. Select to enable anti-passback checking between areas. When this setting is enabled the person(s) who do notuse their badge to exit the area will be denied access to all areas even at readers not set for antipassback. When this setting is disabled person(s) who do not use their badge to exit areas will only be blocked against re-entering their last known area or re-entering the facility from outside.

Ignore outside to inside area check

This field is only available for NGP panels. This setting causes readers to allow entry from outside for person(s) who did not use their badge to exit the facility. This option does not override other anti-passback conditions.

Auto reset

This field is only available for NGP panels. Select the amount of time that anti-passback will be limited after each cardholder is granted access.

User Counting

This field does not appear when using global anti-passback. This section allows you to configure User Counting options.

Interlock all doors in area

This field does not appear when using global anti-passback. Select to enable an interlock area. In a situation where a controlled area is needed, readers in the area can be interlocked. This can be configured using areas. In an interlocked area, only one door may be opened at a time. For any door in the area, if the door strike is active or the door is open, no other door may be opened to leave or enter the area. Any additional request for access will be denied when the interlock is in this busy state.

Two man control

The options in this drop-down are and may differ depending on the panel you are using:

- **None**: No Two man control is used
- **Standard**: If selected, at least two cardholders (if any) must be in the area at all times. The first person attempting access can't get in until the second person attempts access. The last two people to leave the area must leave together.
- **Special 1-Man**: In the Special 1-Man Mode, a special “Team Member” is configured to be the “Area” or “Assigned” owner to a specific area. This “Area Owner” must be the first individual to enter the area and the last individual to exit the area. Once the assigned Area Owner is inside the area, other Team Members or Supervisors are allowed to enter the area. When the assigned Area Owner is in the area and a Supervisor attempts access, a strobe inside the area fires and enables the door release push-button within the room. Individuals who are classified as Others are not allowed access to the area when in this mode.
- **Special 2-Man**: In the Special 2-Man Mode, the first two individuals into the area must be Team Members and the last two individuals to leave the area must also be Team Members. Once two Team Members are inside the area, additional Team Members or Supervisors are allowed access. When a Supervisor attempts access and there are at least two Team Members in the area, a strobe inside the area fires and enables the door release push-button within the room. Individuals who are classified as Others are not allowed access to the area when in this mode. The last two individuals who leave the area must be Team Members.

Note: The special 1-man and special 2-man modes for two man control are only available for local Lenel areas on panels that are configured for special area rules. The two man control option is not available at all for global areas and not available for NGP panels.

For more information please refer to Appendix G: Special Two-Man Rule on page 1435.

Maximum occupancy

This field does not appear when using global anti-passback. Indicates the maximum number of cardholders allowed in the area at any one time. Once this capacity has been reached, the software closes the area and no cardholders can enter it until someone exits.

Close area

This field does not appear when using global anti-passback. If selected, an “Area Closed” event will be triggered in Alarm Monitoring. Cardholders will still be granted access unless you have completed the Area closed rules section of this form. When the area is closed, cardholders can not enter the area unless they are anti-passback exempt.

Counting Mode

This field is only available for NGP panels. The method of counting users in the area. Choices include:

- **Normal** - The system counts each cardholder entering and leaving.
- **Special** - The system counts each cardholder entering the area and subtracts that cardholder from the last known area they were known to occupy.
- **Blind Count** - The stystem counts each time a cardholder is accepted even if the same cardholder is presented more than once.

Reset Before in Schedule

This field is only available for NGP panels. Select the time the area user-count is automatically reset. The time is chosen by how many hours before the schedule is configured to begin.

Reset when area is disarmed

This field is only available for NGP panels. Enable to reset the user-count when the area is disarmed.

Reset when area is armed

This field is only available for NGP panels. Enable to reset the user-count when the area is armed.

Occupancy Actions

This section is only available for non-NGP panels. This section allows you to configure the Occupancy Actions.

Function list

This section is only available for non-NGP panels. This section is used to link the built-in occupancy control commands to lists of actions defined in Local I/O Function Lists. This feature is part of the application’s global event programming capability. Select the local I/O function list to link to this area’s occupancy levels.

Minimum Occupancy

This section is only available for non-NGP panels and when using local anti-passback. Indicates the maximum number of cardholders allowed in the area at any one time. Once this capacity has been reached, the software closes the area and no cardholders can enter it until someone exits.

Maximum occupancy

The number of users that can be present with the area still being considered empty.

Activity Detection

Activity detection uses the time interval specified in **Timeout**. However, if Extended Auto Arm is configured for arming on area inactivity, a 2-minute delay is built in to avoid frequent arming and disarming.

For example:

An area is armed and area inactivity is detected. If a user then disarms the area, automatic re-arming will be delayed for at least 2 minutes or for the **Arming delay** interval if it is greater than 2 minutes. Such delayed re-arming allows the user to open the door and trigger activity detection even if the **Arming delay** interval is for a very short duration.

On the other hand, if the area is disarmed and active, inactivity detection and arming use the **Timeout** and **Arming delay** intervals exclusively without any 2-minute delays.

For more information, refer to section Extended Auto Arm on page 766.

Timeout

This field is only available for NGP panels. Allows disabling the activity detection for each area or setting the maximum duration between activity detections. The status is then reset if no activity is detected for this duration.

Include entry/exit (EE) route inputs

This field is only available for NGP panels. Enable to montior the entry/exit route for the area.

Include door openings

This field is only available for NGP panels. Enable door openings to cause alarms.

Alarm on no activity

This field is only available for NGP panels. Enable to cause an alarm to be generated if a timeout occurs without activity being detected.

Add

Used to add an area.

Modify

Used to change an area.

Delete

Used to remove an area.

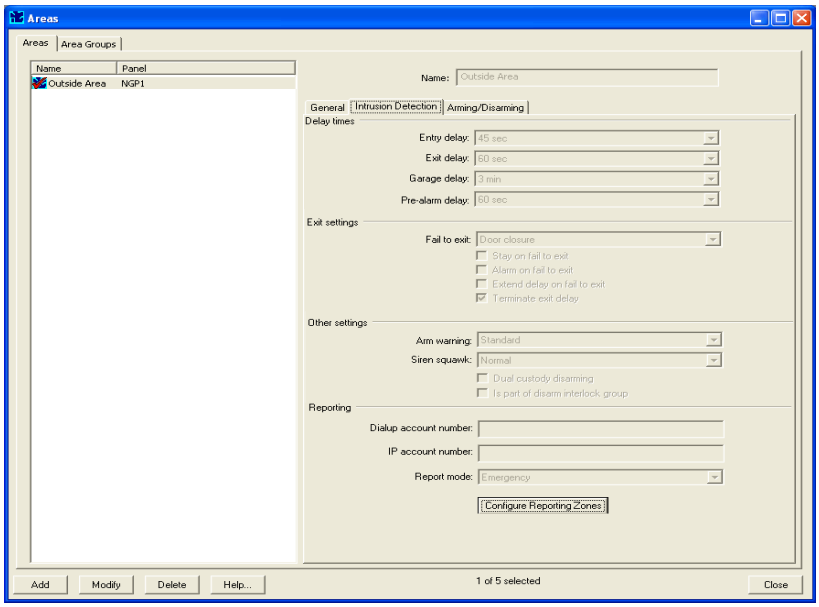
Help

Displays online assistance for this form.

Close

Closes the Areas folder.

Areas Form (Intrusion Detection Sub-tab)



Note: The Intrusion Detection sub-tab is available if an area for an NGP intrusion panel is selected. For more information, refer to Add an Area to an NGP Access Panel on page 1572.

Listing window

Lists currently defined areas and the access panel/segment associated with each.

Name

Specify a name for this area. You can enter a name containing a maximum of 32 characters.

Delay Times

This section allows you to configure the Delay Times options.

Entry Delay

Select the duration that monitoring of the entry point is delayed to allow an authorized entrant to disarm the system.

Exit Delay

Select the duration that monitoring of the exit point is delayed to allow an authorized entrant to exit after arming the keypad.

Garage Delay

Select the duration that monitoring of the garage delay point is delayed to allow an authorized entrant to disarm the keypad.

Extended Delay

Select the duration that monitoring of the extended delay point is delayed to allow an authorized entrant to disarm the keypad.

Pre-Alarm Delay

Select the duration that the system waits before transmitting alarms from this area to the system.

Exit Settings

This section allows you to configure the Exit Settings options.

Fail to Exit

Configures whether a door closure or tripping an exit confirmation button is considered a cardholder exiting the area after it was armed manually. If an exit is not detected the area will not be armed. Choices are:

- **Door Closure** - A door closure is considered a cardholder exiting.
- **Exit Button** - A tripping of an exit button is considered a cardholder exiting.
- **Door Closure or Exit Button** - Both a door closure and tripping of an exit button is considered a cardholder exiting.
- **None** - Neither a door closure and tripping of an exit button is considered a cardholder exiting.

Stay on fail to exit

When enabled, the area automatically switches to stay mode if an exit is not detected after the area was armed manually.

Alarm on fail to exit

When enabled, an alarm to be triggered if an exit is not detected after the area was armed manually.

Extended delay on fail to exit

When enabled, when a fail to exit alarm is triggered the exit delay will be extended by two minutes.

Terminate exit delay

When enabled, the exit delay is truncated when the door closes after the users arms the area and exits.

Other Settings

This section allows you to configure the Other Settings options.

Arm Warning

Select how the system will behave when arming an area while input points are active such as having a door open. Choices are:

- **Standard** - No warning tones and no prompts are given to bypass the inputs.
- **Warning Tones during exit delay** - A warning tone is given until the end of the exit delay.
- **Warning Tones continuous** - A continuos warning tone is given until it is silenced.
- **Warning Tones continuos & blocked arming** - A warning tone is given until it is silenced and the area will not arm.

Siren Squawk

Select if siren outputs for the area will be pulsed briefly when the area is armed and/or if the area is not armed at the scheduled closing time. Choices are:

- **None** - No siren pulse is activated.
- **On Arming** - A siren pulse is activated when an area is armed.

Dual custody disarming

When enabled, two authorized users need to present their badges and/or PINs to disarm an area.

Is part of disarm interlock group

When enabled, the area is set as an interlocked area. Only one area that is part of an interlock group can be disarmed at a time.

Reporting

This section allows you to configure the reporting settings. These settings determine if the area reports should be sent to the central station.

Dialup account number

Enter the dialup account number of the central station where reports will be sent.

IP account number

Enter the IP account number of the central station where reports will be sent.

Report mode

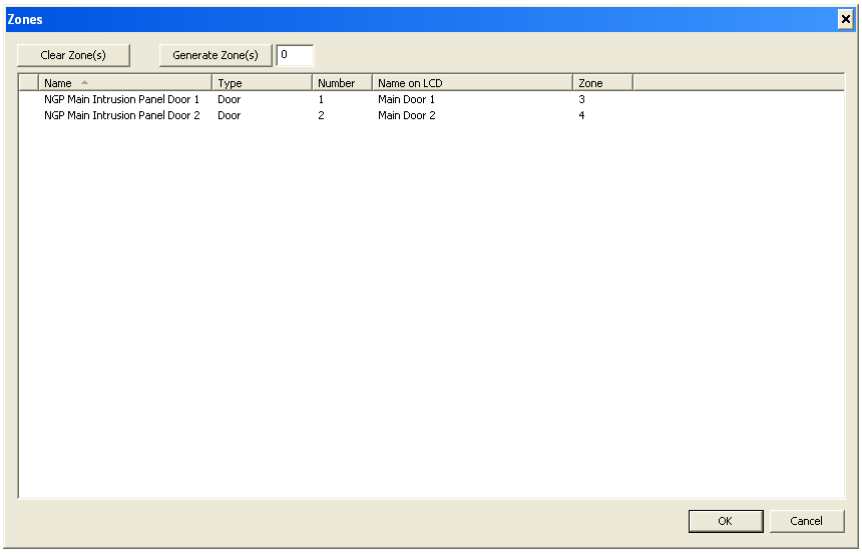
Determines when reports are transmitted. Select:

- **Emergency** - reports are transmitted when the panel is considered to be in trouble or there is an alarm condition while the area was armed.
- **Full** - reports are always transmitted.

Configure Reporting Zones

Click this button to view or configure Central Station reporting zones for the inputs and doors in the selected area. For more information, refer to Add an Area to an NGP Access Panel on page 1572.

Zones Dialog



Listing window

Presents a list of input and door zone assignments for a given area. By default, the list is sorted by device **Name** in ascending order. In addition, zone information includes:

- The first column displays the update status of each zone:

Status icon	Description
	Indicates the zone information for the device was modified.
	Indicates a zone number conflict for the device. Zone number changes are not saved unless the duplicate zone numbers are resolved. Zones numbers must be unique within an area.

- **Type** - Displays the device type (Input, Door, or Aux Input).
- **Number** - Displays the Reader number or Input number of the device.
- **Name on LCD** - Identifies the name of the device displayed on the LCD. This field is editable.
- **Zone** - Identifies the reporting zone number of the device. This field is editable and allows you to assign up to 998 zones *per* area including 128 doors and 512 inputs.

Clear Zone(s)

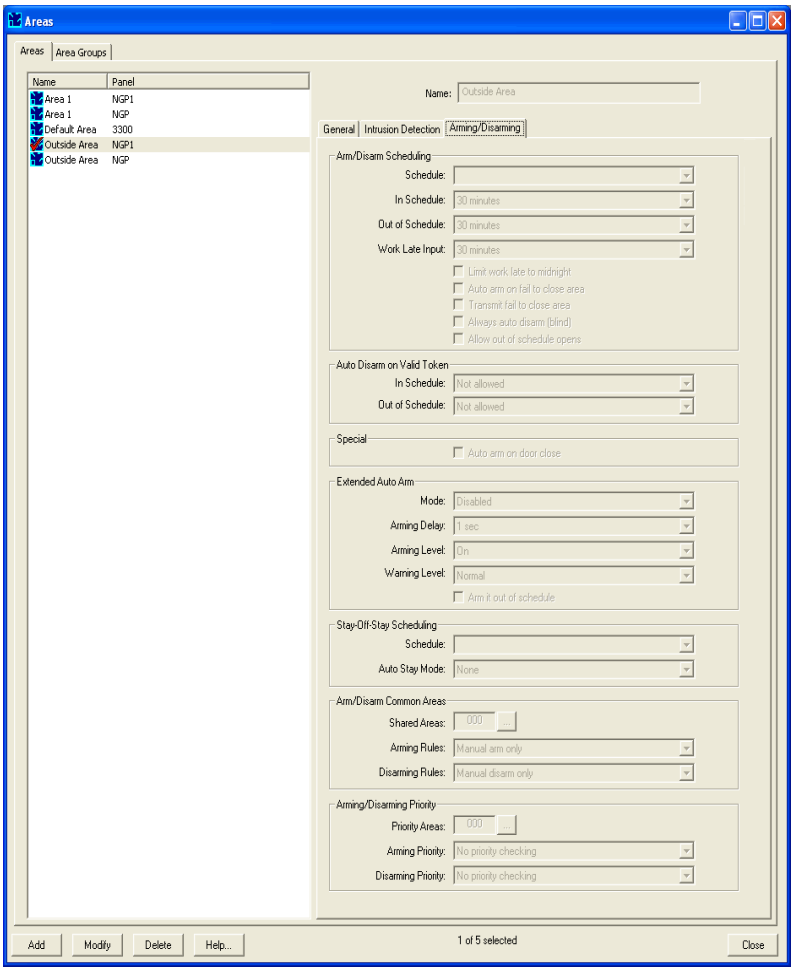
Click to set all device zone numbers to zero (0).

Generate Zone(s)

Click to generate zone numbers for multiple devices.

Before generating zone numbers, enter a beginning zone number in the field to the right of this button, and then select the devices you want to update. When you click [Generate Zone(s)], the zone number of the selected devices will be updated in sequence to the next available zone number starting from the number entered.

Areas Form (Arming/Disarming Sub-tab)



Note: The Arming/Disarming sub-tab is available if an area for an NGP panel is selected. For more information, refer to Add an Area to an NGP Access Panel on page 1572.

Listing window

Lists currently defined areas and the access panel/segment associated with each.

Name

Specify a name for this area. You can enter a name containing a maximum of 32 characters.

Arm/Disarm Scheduling

This section allows you to configure the Arm/Disarm Scheduling options.

Schedule

Select the schedule to be associated with this area. At the scheduled closing time the area keypads will beep to remind users to either arm the area and exit or delay the closing time. If neither of these actions occur an alarm can be transmitted and/or the area can be armed automatically.

Notes: When you select an item from the **Schedule** drop-down, you also need to select one or more of the applicable check box items within the Arm/Disarm Scheduling section. Simply selecting a schedule will not do anything on its own. In addition, if a schedule is

used along with an automatic arm/disarm option, when the schedule begins (based on the **In schedule** value) the area will be disarmed. When the schedule ends (based on the **Out of schedule** value) the area will be armed.

If you want to enable auto arming, you also need to select the **Auto arm on fail to close area** check box. For auto disarming, you need to select the **Always auto disarm (blind)** check box to enable this function.

In schedule

The length of time before the area will automatically re-close after being disarmed inside of the schedule. This allows limiting the time that authorized users can remain in the area during the schedule.

Out of schedule

The length of time before the area will automatically re-close after an area is disarmed outside of the schedule.

Work late input

When a user presses a work-late button in this area (during the pre-arm cycle), the scheduled closing time will be delayed for duration set in this field.

Limit work late to midnight

When enabled, a user is not able to extend the work schedule past midnight in this area.

Auto arm on fail to close area

When enabled, the area will ato-arm at the scheduled closing time.

Transmit fail to close area

When enabled, an alarm is generated if the area has not been armed at the scheduled closing time.

Always auto disarm (blind)

When enabled, when the area's schedule becomes active the area will fully disarm automatically. If not enabled, the area will remain armed until it is disarmed either manually or when someone is granted entry.

Allow out of schedule opens

When enabled, users without authority are able to gain entry and/or disarm the area outside of its open/close schedule and adjust the area closing time after their schedule has expired.

Auto Disarm on Valid Token

This section allows you to configure the Auto Disarm on Valid Token options.

In Schedule

Select whether or not auto-disarming will occur for this area while the area schedule is active.

Out of Schedule

Select whether or not auto-disarming will occur for this area while the area schedule is not active.

Special

This section allows you to configure the Special options.

Auto arm on door close

Select to auto arm the door once it is closed.

Extended Auto Arm

This section allows you to configure the Extended Auto Arm options.

Mode

Select the mode of the extended auto arm.

Arming Delay

Select a value here to have the preceding auto-arm (mode) selection delayed (not occur) for a set period of time.

Arming Level

This sets the arming level for activity or user-count based auto-arming (arm to 'Stay', or fully arm to 'On'). Choices are:

- **Stay**: Only perimeter sensors monitored.
- **ON**: All sensors monitored.

Warning Level

Select the level of warning given. Choices are:

- **Normal** - Normally warns you.
- **Warn if users left in area** - Warns you if any users are left in the area.
- **Block manual arming if users left in area** - Blocks you from manually arming if any users are left in the area.
- **Block all arming if users left in area** - Blocks all arming if any users are left in the area.

Arm if out of schedule

This determines whether or not the activity and 'user-count auto-arming will be limited to only outside of the arming schedule versus any time.

Stay Off Stay Scheduling

This section allows you to configure the Stay Off Stay Scheduling options.

Schedule

A schedule to be associated with automated stay/off/stay arming in this area (also see next setting).

Auto Stay Mode

Specifies that the area will automatically switch from Stay to Off and then Off to Stay, in-sync with schedule chosen above. This will not occur if the area is fully armed (ON) at the applicable times.

Arm/Disarm Common Areas

This section allows you to configure the Arm/Disarm Common Areas options.

Shared Areas

Select other areas to be shared.

Arming Rules

Select the rules for arming the selected area. Choices are:

- **Manual arm only** - This area can only be armed manually.
- **Auto arm if all areas armed** - This area is auto armed if all other shared areas are armed.
- **Auto arm if any shared area armed** - This area is auto armed is any shared area is armed.

- **Arm all shared areas if common area armed** - When this area is armed all shared areas are also armed.

Disarming Rules

Select the rules for disarming the selected area. Choices are:

- **Manual disarm only** - This area can only be disarmed manually.
- **Auto disarm if all areas disarmed** - This area is auto disarmed if all other shared areas are disarmed.
- **Auto disarm if any shared area disarmed** - This area is auto disarmed if any shared area is disarmed.
- **Disarm all shared areas if common area disarmed** - When this area is disarmed all shared areas are also disarmed.

Arming/Disarming Priority

This section allows you to configure theArming/Disarming Priority options.

Priority Areas

Assign a priority values for specific areas such that each area can only be armed or disarmed in the order of their set priority value (1, 2, 3,..., 15). Areas set to the same priority value can be armed and/or disarmed in any order relative to each other.

Arming Priority

Allows assigning priority values for specific areas such that each area can only be armed in the order of their set priority value.

Disarming Priority

Allows assigning priority values for specific areas such that each area can only be disarmed in the order of their set priority value.

Add

Used to add an area.

Modify

Used to change an area.

Delete

Used to remove an area.

Help

Displays online assistance for this form.

Close

Closes the Areas folder.

Areas Form Procedures

The following procedures can be performed on this form.

Add an Area

IMPORTANT: Depending on the area type and the access panel being used you will see different options to configure. If you are adding an area to an NGP panel refer to Add an Area to an NGP Access Panel on page 1572.

1. Select ***Areas*** from the ***Access Control*** menu. The Areas folder opens.
2. Select the Areas tab.
3. Click [Add].
4. A dialog appears asking you to select the type of area to create.
   a. Select the type of area.
   b. Select the panel(s) to be associated with the area.
   c. Click [Select area type].
5. In the **Name** field, type a descriptive name for this area.
6. In the **Panel** field, select the access panel with which this area will be associated.
7. If your system/segment is configured for mustering, select an **Area type**.
8. Configure any **Anti-Passback** options if the specified access panel supports them.
9. Configure any **User Counting** options if the specified access panel supports them.
10. If you wish to link a function list to this area, complete the Occupancy Actions section.
11. Click [OK].

Modify an Area

1. In the listing window, select the name of the area to be changed.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete an Area

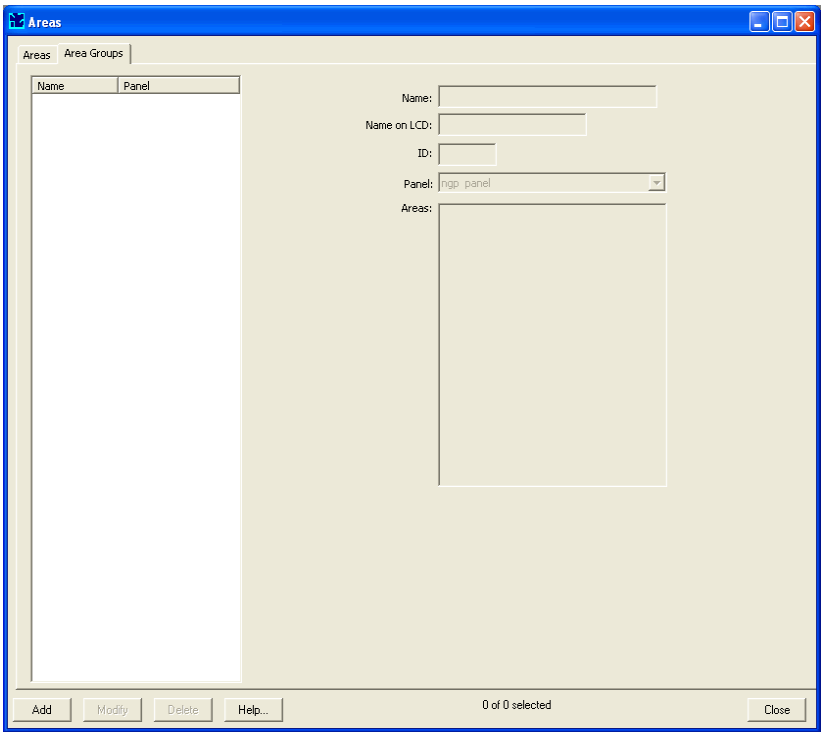
1. In the listing window, select the name of the area to be deleted.
2. Click [Delete].
3. Click [OK].

Configure an Interlocked Area

1. On the Areas form, Add an Area on page 768.
   a. For the panel, you may only select an LNL-2220 or LNL-3300 for this functionality.
   b. Select the **Interlock all doors in area** check box.
2. In the Readers folder, on the Anti-Passback form, select the reader that is to be used to gain access to the area.
   a. From the **Area entering** drop-down, select the name of the interlocked area.
   b. Repeat this step for any readers to be configured for entering the interlocked area.
3. Select the reader that is to be used to exit the area.
   a. From the **Area leaving** drop-down, select the interlocked area.
   b. Repeat this step for any readers to be configured for exiting the interlocked area.

4. Click [OK].

Area Groups Form



Note: The Area Groups Form only appears if an area for an NGP panel is selected.

Listing window

Lists currently defined areas and the access panel/segment associated with each.

Name

Specify a name for this area group. You can enter a name containing a maximum of 32 characters.

Name on LCD

The name as it will appear on the LCD reader display.

ID

Enter the ID as displayed on your NGP hardware. The ID acts as a unique identifier for the hardware.

Panel

Select the panel that the areas are associated with.

Areas

Select the area(s) to add to the area group.

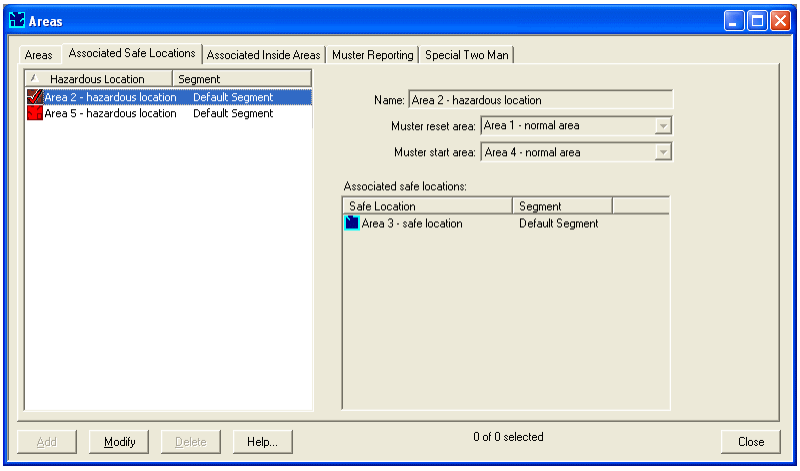
Add an Area Group

For more information, refer to Add an Area Group on page 1573.

Associated Safe Locations Form

Associated safe locations are areas that are specified by a given Hazardous Location. When an emergency incident occurs in a hazardous location, a muster report is generated. This report lists all of the cardholders that are currently in the hazardous location. Cardholders can register in a safe location by checking in at a specified muster reader.

Once a cardholder has registered in a safe location, which is specified on this form, they are then removed from the muster report. The muster report then becomes a report of all of the cardholders who were in the hazardous location at the time of the emergency incident, but who have failed to register at a safe location.



Listing window

Displays a list of all currently defined areas with the “Hazardous location” area type. Areas are configured on the Areas form of this folder.

Name

Displays the name of the area which is selected in the listing window.

Muster reset area

Select a muster reset area. A muster reset area is an area where cardholders can be optionally moved to (from the safe location). A muster reset action indicates that the system is no longer in muster mode. Muster reset areas can be an outside area (when safe locations are outside of the hazardous location) or back into the hazardous location (when safe locations are inside of the hazardous location). Choices include all currently defined areas with either the “Hazardous location” or “Normal area” area type.

Muster start area

If muster mode is manually started, select the area where it is to be started from.

Associated safe locations listing window

In view mode, displays a list of currently defined safe location areas that have been associated with the area selected in the main listing window. In modify mode, displays a list of all currently

defined areas with the “Safe location” area type. Areas are configured on the Areas form of this folder.

Modify
Click this button to configure an associated safe location.

Help
Click this button to display online assistance for this form.

Close
Click this button to close the Areas folder.

Associated Safe Locations Form Procedures

The following procedures can be performed on this form.

Configure an Associated Safe Location

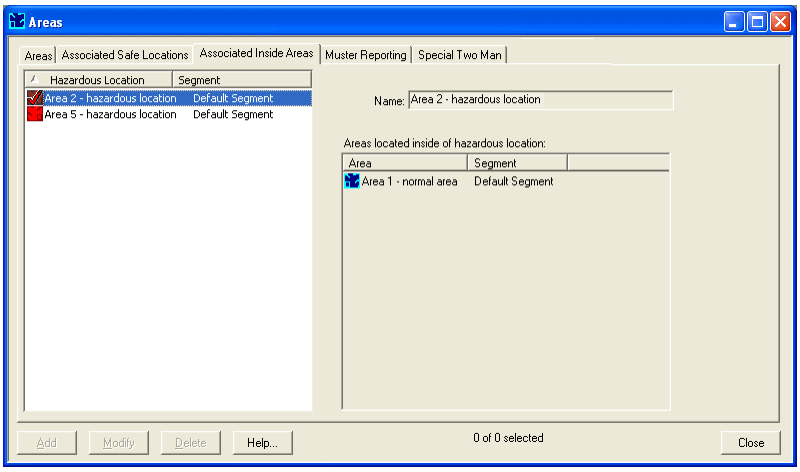
1. Select ***Areas*** from the ***Access Control*** menu. The Areas folder opens.
2. Select the Associated Safe Locations tab.
3. Click on an area in the listing window to select it. The name of the selected area will be displayed in the **Name** field.
4. Click [Modify].
5. If you want to associate the selected area with a muster reset area, select an area from the **Muster reset area** drop-down list.
6. If you want to associate the selected area with a muster start area, select an area from the **Muster start area** drop-down list.
7. Click on an area from the Associated safe locations listing window to select it.

Note: You can select multiple entries.

8. Click [OK].

Associated Inside Areas Form

The associated inside areas are areas specified to be inside a hazardous location. Cardholders located in these areas are put into a mustering report during an emergency until they reach a safe location and use their badge on a predetermined reader.



Listing window

Displays a list of all currently defined areas with the “Hazardous location” area type. Areas are configured on the Areas form of this folder.

Name

Displays the name of the area which is selected in the listing window.

Areas located inside of hazardous location listing window

In view mode, displays a list of currently defined inside areas that have been associated with the area selected in the main listing window. In modify mode, displays a list of all currently defined areas with the “Normal area” area type. Areas are configured on the Areas form of this folder.

Add

This button is not used.

Modify

Click this button to configure an associated inside area.

Delete

This button is not used.

Help

Click this button to display online assistance for this form.

Close

Click this button to close the Areas folder.

Associated Inside Areas Form Procedures

The following procedures can be performed on this form.

Configure an Associated Inside Area

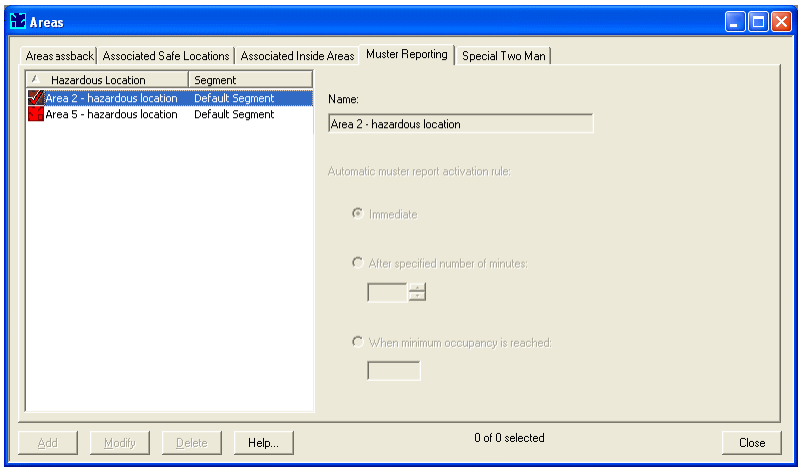
1. Select ***Areas*** from the ***Access Control*** menu. The Areas folder opens.
2. Select the Associated Inside Areas tab.

3. Click on an area in the listing window to select it. The name of the selected area will be displayed in the **Name** field.
4. Click [Modify].
5. Click on an area from the Areas located inside of hazardous location listing window to select it.

Note: You can select multiple entries.

6. Click [OK].

Muster Reporting Form



Listing window

Displays a list of all currently defined areas with the “Hazardous location” area type. Areas are configured on the Areas form of this folder.

Name

Displays the name of the area which is selected in the listing window.

Immediate

Select this radio button if you want a Muster report to be run immediately following an emergency incident.

After specified number of minutes

Select this radio button and enter a number if you want a Muster report to be run after a specified number of minutes after an emergency incident.

When minimum occupancy is reached

Select this radio button and enter a number if you want a Muster report to be run after a minimum occupancy is reached in a hazardous location after an emergency incident.

Add

This button is not used.

Modify

Click this button to configure muster reporting.

Delete
This button is not used.

Help
Click this button to display online assistance for this form.

Close
Click this button to close the Areas folder.

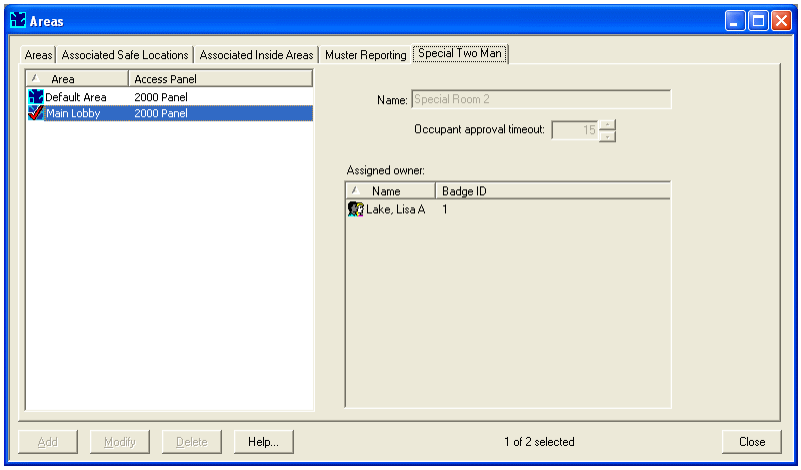
Muster Reporting Form Procedures

The following procedures can be performed on this form.

Configure Muster Reporting

1. Select ***Areas*** from the ***Access Control*** menu. The Areas folder opens.
2. Select the Muster Reporting tab.
3. Click on an area in the listing window to select it. The name of the selected area will be displayed in the **Name** field.
4. Click [Modify].
5. Choose one of the following automatic muster report activation rules:
   - **Immediate** - select this radio button if you want a muster report to be run immediately following an emergency incident.
   - **After a specified number of minutes** - select this radio button and enter a number if you want a muster report to be run after a specified number of minutes after an emergency incident.
   - **When minimum occupancy is reached** - select this radio button and enter a number if you want a muster report to be run after a minimum occupancy is reached in a hazardous location after an emergency incident.
6. Click [OK].

Special Two Man Form



Listing window

Displays a list of all currently defined areas with the "Special Two Man" option enabled. Areas are configured on the Areas form of this folder.

Name

Displays the name of the area which is selected in the listing window.

Occupant approval timeout

Refers to the timeout used for the strobe authorization. The occupant approval timeout will have a valid range of 1 to 255 seconds. For more information, refer to Configure the Areas for Special Two-Man Rule on page 1440.

Assigned owner

The area owner is configured here and is used when the area is in 1-man mode. The area owner is a team member who, once in the area, allows the other team members to enter without approval from inside. For more information, refer to Configure the Areas for Special Two-Man Rule on page 1440.

Configure Special Two Man

1. Select ***Areas*** from the ***Access Control*** menu. The Areas folder opens.
2. Select the Special Two Man tab.

Note: For the Special Two Man tab to appear you must first have the Special Two-Man Rule enabled. For more information, refer to Special Two-Man Rule on page 1435.

3. Click on an area in the listing window to select it. The name of the selected area will be displayed in the **Name** field.
4. Click [Modify].
5. Set the **Occupant approval timeout** to a number you wish (between 1-255).
6. If you want, choose an Assigned owner by selecting the name of the team member.
7. Click [OK].

CHAPTER 36

Groups Folder

The folder contains two forms, the Mask Groups form and the Device Groups form.

The Groups folder is displayed by selecting ***Groups*** from the ***Access Control*** menu, or by selecting the Groups toolbar button.

The Groups folder contains forms with which you can:

- Create groups that enable you to mask or unmask multiple alarm inputs and readers simultaneously.
- Create groups that enable you to configure and control intrusion groups.
- Define device groups consisting of one or more readers, (alarm or reader) inputs, or (alarm or reader) output devices.

  Each device event assignment can belong to one and only one alarm mask group.
- (Lenel hardware only) Assign global I/O function lists that are invoked when the selected mask group is activated or deactivated.
- (LNL-2220 and LNL-3300 hardware only) Configure intrusion mask groups which allow intrusion point configuration and are able to execute local I/O functions based on intrusion group state transitions.

  Up to 64 mask groups are configurable per access panel.

  When configuring door request, door forced, and door held events with an intrusion mask group, be aware that only one of those events can be assigned to an intrusion mask group.

Mask Groups Form Overview

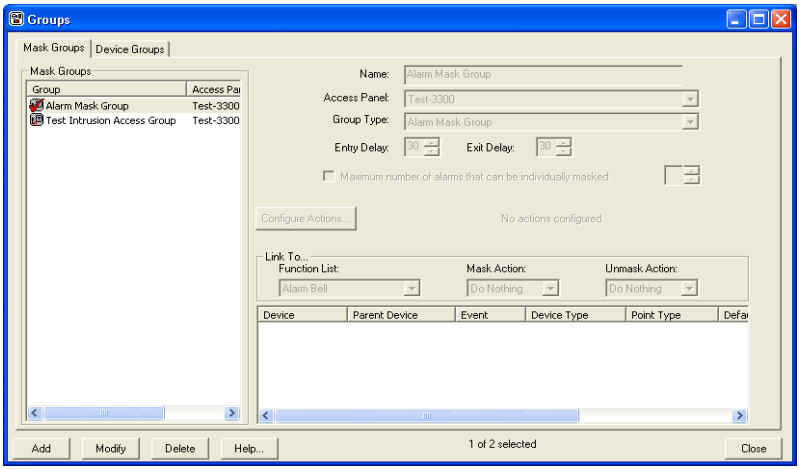
There are two types of mask groups:

Alarm Mask Group. Alarm mask groups are used to control an alarm's reporting behavior. Alarm mask groups have two option available for configuring an input: mask and unmask. When an alarm is masked it is disabled and prevented from signaling an alarm. When an alarm is unmasked, it is enabled and alarms are able to be reported. Alarm Mask Groups support a maximum of 128 inputs.

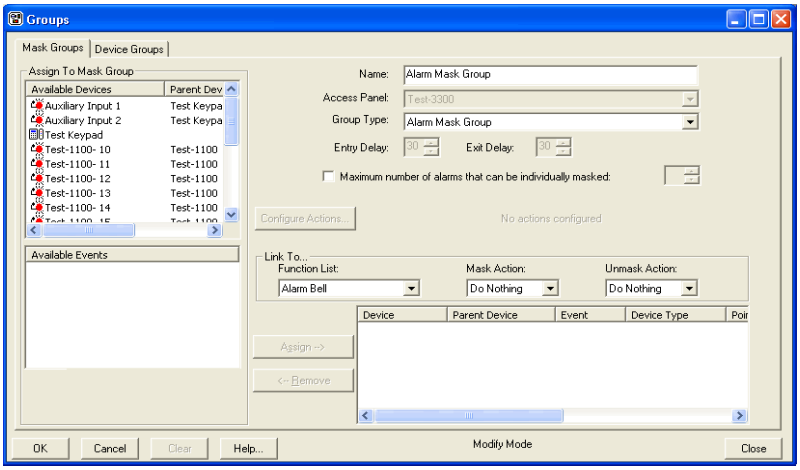
Intrusion Mask Group. An intrusion mask groups are set much like a home-security system. It is either armed or disarmed. What alarm is reported depends on the different point type configured.

Mask Groups Form

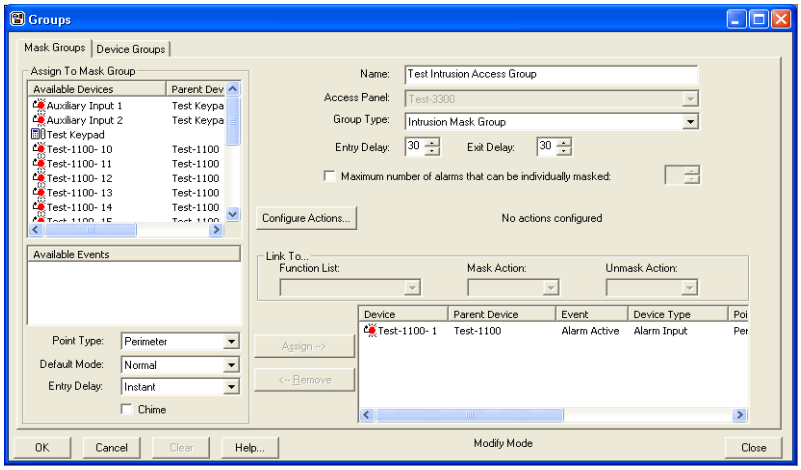
Mask Groups Form (View Mode)



Mask Groups Form (Alarm Mask Group Modify Mode)



Mask Groups Form (Intrusion Mask Group Modify Mode)



Intrusion Mask Group Permissions

The following user permissions must be enabled for a user to interact with intrusion mask group related alarms in Alarm Monitoring.

The following permissions can be configured in System Administration by selecting the menu option ***Administration*** **>** ***Users*** and navigating to Monitor Permission Groups > Control.

- Mask (Disarm) mask groups - gives permissions to disarm an intrusion mask group from Alarm Monitoring.
- Unmask (Arm) mask groups - gives permissions to enable arm away, arm stay, or arm stay instant intrusion mask groups in Alarm Monitoring.
- Mask alarms and inputs - gives permissions to issue the bypass, disable or restore commands for inputs belonging to an intrusion mask group.

The following permission can be configured in System Administration by selecting the menu option ***Administration*** **>** ***Users*** and navigating to System Permission Groups > Access Control Hardware.

- Mask Groups - gives permissions in order to add, modify, and/or delete intrusion mask groups

Groups Folder - Mask Groups Form Fields

Mask Groups

(displayed in view mode only) Lists all currently defined mask groups, and the access panel associated with each.

Name

Indicates the name of the mask group.

Access Panel

The access panel that contains the devices in the mask group. Each mask group is associated with only one access panel.

Group Type

Used to define what type of mask group you are creating. Choices include:

– Alarm Mask Group

- Intrusion Mask Group

Some fields on the Mask Groups form can only be modified when configuring an intrusion mask group

Entry Delay

(Intrusion Mask Groups only) The amount of time in seconds a cardholder is allowed to enter a facility before an alarm will be reported for the intrusion mask group.

Exit Delay

(Intrusion Mask Groups only) The amount of time in seconds a cardholder is allowed to leave a facility when either the Arm Away or Arm Stay arming modes are set for an intrusion mask group.

Maximum Number of Alarms That Can be Individually Masked

Select this check box to limit the number of alarms that someone can mask individually. You specify the number in the **max. number** field.

max. number

Activated when the **Maximum Number of Alarms That Can be Individually Masked** check box is selected. Specifies the number You can choose a number in the range of 0 through the current number of entries in the assignment window. The default is the current number of entries.

Configure Actions

Opens the Mask Group Function Links window which allows you to configure local I/O function lists to be executed when an intrusion mask group transitions into and out of various states.

Link To

(Alarm Mask Groups only) This section is configurable for Lenel hardware only. Includes the **Function List**, **Mask Action**, and **Unmask Action** drop-down list fields.

Function List

(Alarm Mask Groups only) Selects the function list that will be affected by the Mask Action (when this alarm mask group is activated) and by the Unmask Action (when this alarm mask group is deactivated). The function list must have already been defined for the selected access panel. Function lists are defined using the Global I/O Function Lists form of the Global Input/ Output folder.

Mask Action

(Alarm Mask Groups only) Indicates the action to be performed on the selected function list when the alarm mask group is activated; i.e., when the group's mask count is other than zero. The action is performed whenever the group's mask count changes. For example, if the group count increments from 0 to 1 and then from 1 to 2, the Mask Action will be performed twice on this function list, once for each increment.

Unmask Action

(Alarm Mask Groups only) Indicates the action to be performed elected function list when the alarm mask group is deactivated; i.e., when the group's mask count equals zero (0).

Point Type

(Intrusion Mask Groups only) Used to select what kind of input that is monitored for an intrusion mask group. Choices include:

- 24 Hour - Activates an alarm condition for the intrusion mask group regardless of arming mode. The 24 Hour point is used when an area needs to be constantly monitored. Examples of use would be to monitor fire conditions.

- Interior - Used to monitor a specific area within a facility. An interior point will activate an alarm only when an intrusion mask group is in an Armed Away arming mode.
- Perimeter - Used to monitor an area outside of a facility. An example being an alarm on a window to detect a break in. A perimeter input activates an alarm only when an intrusion mask group is in the Arm Away, Army Stay or Arm Stay Instant arming modes.

Default Mode

(Intrusion Mask Groups only) Used to select the supervision mode applied to the Point Type. Choices include:

- Normal - Select to monitor for alarms normally.
- Disabled - Select to disable alarms for the intrusion mask group.

Entry Delay

(Intrusion Mask Groups only) Used to select what, if any, delay will be applied to alarms when entering a facility. Choices include:

- Follower - Input is masked during an entry delay.
- Instant - Select to have no delay in alarm reporting once a cardholder enters a facility.
- Trigger - Select to have a delay in alarm reporting once a cardhodler enters a facility. The number of seconds in the delay is entered in the Entry Delay field.

Chime

(Intrusion Mask Groups only) Select to enable the command keypad to produce an audio signal. A command keypad template needs to be configured and the **Chime on point active** field selected for the chime to work properly. For the audio to work correctly the command keypad needs to be assigned to a reader capable of producing audio.

assignment window

Lists all device + event pairs that the mask group currently includes. An icon precedes each alarm input entry. An icon precedes each reader entry.

Assign To Mask Group

(displayed in modify mode only) Includes the Available Devices and Available Events fields.

Available Devices

(displayed in modify mode only) Lists all devices (readers and alarm inputs) that are connected to the selected access panel and that are available for inclusion in the mask group. Each entry includes the device name, the parent device (such as the access panel to which the device is connected), and the device type (such as “reader”). An icon precedes each alarm input entry. An icon precedes each reader entry.

Available Events

(displayed in modify mode only) Lists all unassigned events for the selected reader or alarm input. Available choices vary with the device type. An icon precedes each entry.

Assign

(displayed in modify mode only) Assigns the selected reader or alarm input and the selected event to the mask group. Specifically, it adds the device + event pair to the assignment window.

Remove
(displayed in modify mode only) Removes the selected device + event pair from the assignment window, and inserts the event entry back into the Available Events window.

Add
Used to add an mask group.

Modify
Used to change an mask group.

Delete
Used to delete an mask group.

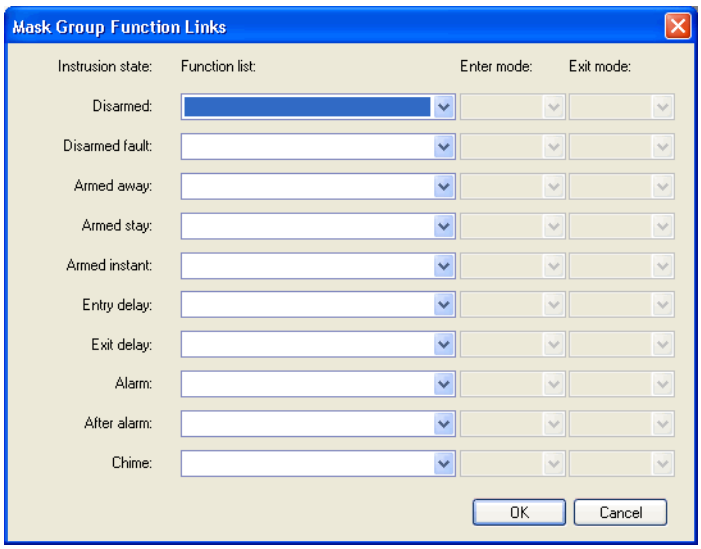
Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the Groups folder.

Mask Group Function Links Window

The Mask Group Function Links window allows you to configure local I/O function lists to be executed when an intrusion mask group transitions into and out of various states.



Disarmed
Indicates that points in the intrusion state are normal with no faults.

Disarmed fault
Indicates that a point in the intrusion state is in a fault state.

Armed away
Indicates an intrusion mask group arming state

Armed stay
Indicates an intrusion mask group arming state

Armed instant
Indicates an intrusion mask group arming state

Entry delay
Indicates that an intrusion mask group is currently armed and an entry delay is in progress.

Exit delay
Indicates that an intrusion mask group is transitioning from the disarmed to armed state.

Alarm
Indicates that an input assigned to the mask group has activated and caused an alarm condition

After alarm
A state that indicates an alarm acknowledgement for an intrusion mask group.

Chime
Indicates how the local I/O is executed when a chime condition occurs.

Function list
Items listed here are Local I/O functions that are configured in the Local I/O folder. For more information, refer to Chapter 37: Local I/O Folder on page 791.

Enter mode
Indicates how the local I/O is executed when entering the intrusion state.

Exit mode
Indicates how the local I/O is executed when exiting the intrusion state.

Mask Groups Form Procedures

Use the following procedures on this form.

Add an Alarm Mask Group

IMPORTANT: Alarm Mask Groups support a maximum of 128 inputs.

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for this alarm mask group.
3. From the **Access Panel** drop-down list, select the access panel for which you want to create an alarm mask group. Readers and alarm inputs connected to this panel will then be listed in the Available Devices window.
4. Select a device (reader or alarm input) in the Available Devices window. This displays, in the Available Events window, the list of selectable events for that device.
5. Select one or more events from the list. You can add more later if you want.

Note: Because an alarm input has only one assignable event (“Alarm Active”), it is automatically selected.

6. Click [Assign]. The device + event pair will be added to the assignment window. If you selected multiple events, each one will be listed in a separate entry.

Note: If the item you are adding is already defined, it will be updated with any changes.

7. Repeat steps 4-6 for each device to be included in the alarm mask group.
8. To remove a device + event assignment from the group, select the entry in the assignment window, then click [Remove].
9. For these assignments, if you want to restrict the number of alarms that someone can mask individually:
   a. Click on the Maximum Number of Alarms That Can be Individually Masked check box.
   b. In the **max. number** field, use the spin buttons to specify the number.
10. If you are configuring an alarm mask group for Lenel hardware, you can select a function list, and actions to be performed on that list when the group is activated (masked) or deactivated (unmasked).
11. Click [OK]. The name of the alarm mask group will be added to the Alarm Mask Groups window.

Add an Intrusion Mask Group

IMPORTANT: Intrusion Mask Groups support a maximum of 128 inputs.

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for this intrusion mask group.
3. From the **Access Panel** drop-down list, select the access panel for which you want to create an intrusion mask group. Readers and alarm inputs connected to this panel will then be listed in the Available Devices window.
4. From the **Group Type** drop-down list, select **Intrusion Mask Group**.
5. Select a device (reader or alarm input) in the Available Devices window. This displays, in the Available Events window, the list of selectable events for that device.
6. Select one or more events from the list. You can add more later if your wish.

Notes: Because an alarm input has only one assignable event (“Alarm Active”), it is automatically selected.

When configuring door request, door forced, and door held events with an intrusion mask group, be aware that only one of those events can be assigned to an intrusion mask group.

7. Click [Assign]. The device + event pair will be added to the assignment window. If you selected multiple events, each one will be listed as a separate entry.
8. Repeat steps 4-6 for each device to be included in the intrusion mask group.
9. To remove a device + event assignment from the group, select the entry in the assignment window, then click [Remove].
10. For these assignments, if you want to restrict the number of alarms that someone can mask individually:
    a. Click on the Maximum Number of Alarms That Can be Individually Masked check box.
    b. In the **max. number** field, use the spin buttons to specify the number.

11. Click [OK]. The name of the intrusion mask group will be added to the Mask Groups window.
12. In order to execute commands at a command keypad for an intrusion mask group you must first have advanced permission control. To configure this:
    a. Navigate to ***Administration*** > ***System Options*** or if you have a segmented system ***Administration*** > ***Segments*** > ***Segments***.
    b. Click on the User Commands sub-tab.
    c. Click [Modify]
    d. Select **Advanced Permission Control** from the **Intrusion command configuration** drop-down box.
    e. Click [OK].

Modify a Mask Group

1. In the Mask Groups window, select the name of the group you want to change.
2. Click [Modify].
3. Make the changes you want to the fields. The [Clear] button clears all field values.

Note: You cannot change an Access Panel selection because all other selections depend upon it.

4. If you want to modify an existing device + event pair, select an alternative device (reader or alarm input), event(s), Point Type, Default Mode, Entry Delay, and/or Chime.
5. Click [Assign]. If the item you are assigning is already defined, it will be updated with any changes.
6. Click [OK] to save the field changes, or on the [Cancel] button to revert to the previously saved values.

Delete a Mask Group

1. In the Mask Groups window, select the name of the group you wish to delete.
2. Click [Delete].
3. Click [OK].
4. Click [Yes] to confirm.

Configure Actions in the Mask Group Function Links Window

1. In **Group Type**, select **Intrusion Mask Group**.
2. Click [Configure Actions]. The Mask Group Function Links window opens.
3. Configure the options for any or all intrusion states. These include
    a. **Function list** - Items listed here are Local I/O functions that are configured in the Local I/O folder. For more information, refer to Chapter 37: Local I/O Folder on page 791.
    b. **Enter mode** - Select what happens when the function enters the intrusion state.
    c. **Exit mode** - Select what happens when the function exits the intrusion state.
4. Click [OK] to apply the changes.

Device Groups Form

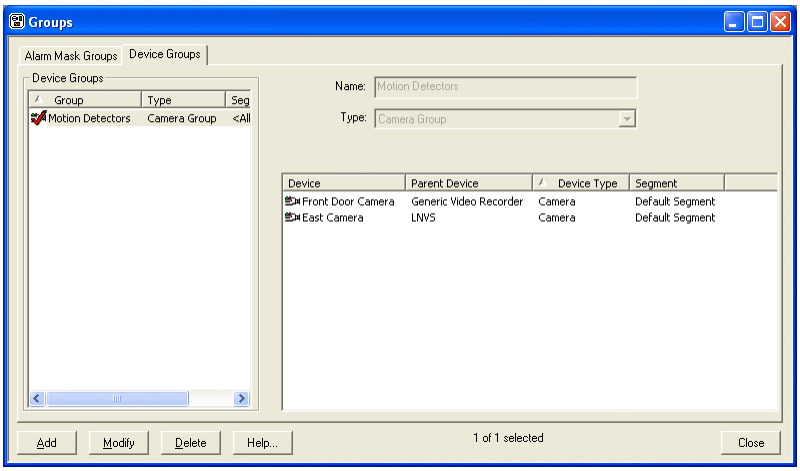
This form is used to define device groups consisting of one or more reader, (alarm or reader) input, (alarm or reader) output, camera, or remote monitor devices.

Notes: A group can contain devices from more than one access panel

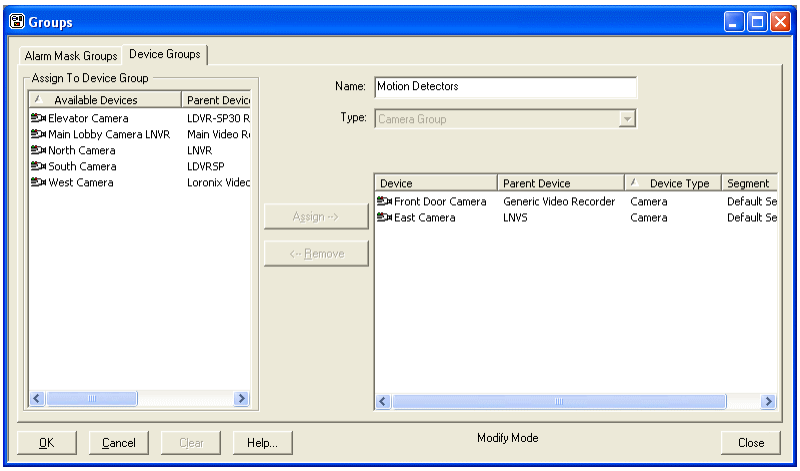
A device can belong to more than one device group

If your system uses segmentation, device groups can be segmented. A device group can belong either to one segment or to all segments. If a device group belongs to only one segment, the group will contain only devices associated with an access panel that was defined for that segment

Device Groups Form (View Mode)



Device Groups Form (Modify Mode)



Device Groups

(displayed in view mode only) Lists all currently defined device groups, and each group's type (reader, input, output, camera, or monitor). An icon precedes each reader group entry. An icon precedes each input group entry. An icon precedes each output group entry. An icon precedes each camera group entry. An icon precedes each monitor group entry.

Name

Indicates the name of the device group.

Type

Select the type of device group. Choices include:

- Reader Group - contains one or more readers that are currently defined in the system
- Input Group - contains one or more alarm panel inputs and/or reader auxiliary inputs. The inputs must be currently defined in the system
- Output Group - contains one or more alarm panel outputs and/or reader auxiliary outputs. The outputs must be currently defined in the system
- Camera Group - contains one or more cameras that are currently defined in the system.
- Monitor Group - contains one or more remote monitors that are currently defined in the system.

Assign To Device Group

(displayed in modify mode only) Lists all currently defined devices of the selected type (readers, alarm inputs, alarm outputs, cameras, or remote monitors) as determined by the **Type** field selection. Offline readers are not available because the purpose of creating device groups is to perform online operations.

Each entry includes:

- the device name
- the parent device (the access panel, alarm panel, or reader to which the device is connected)
- the device type (reader, reader aux input, reader aux output, alarm input, alarm output, camera or remote monitor)

An icon precedes each reader entry. An icon precedes each input entry. An icon precedes each output entry. An icon precedes each camera entry. An icon precedes each remote monitor entry.

Assign

(displayed in modify mode only) Moves the device entry selected in the **Assign To Device Group** field to the assignment window.

Remove

(displayed in modify mode only) Removes the selected device entry from the assignment window, and inserts it back into the Assign To Device Group window.

Assignment window

Lists all devices assigned to the current device group. Each entry includes:

- the device name
- the parent device (the access panel, alarm panel, or reader to which the device is connected)
- the device type (reader, reader aux input, reader aux output, alarm input, alarm output, camera or remote monitor).

An icon precedes each reader entry. An icon precedes each input entry. An icon precedes each output entry. An icon precedes each camera entry. An icon precedes each remote monitor entry.

Add

Used to add a device group.

Modify
Used to change a device group.

Delete
Used to delete a device group.

Help
Displays pertinent help information on screen.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the Groups folder.

Device Groups Form Procedures

Use the following procedures on this form.

Add a Device Group

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for this device group.
3. From the **Type** drop-down list, select the type of device group you want to create. All currently defined devices of this type will then be listed in the Assign to Device Group window.
4. To add a device to the group, select the device entry in the Assign to Device Group window, then click [Assign].

   This moves the selected device from the Assign to Device Group window to the assignment window.
5. Repeat step 4 for each device to be included in the group.
6. To remove one or more devices from the group, select the corresponding entr(ies) in the assignment window, then click [Remove]. The entries will be moved back into the Assign to Device Group list.
7. Click [OK]. The group name will be added to the Device Groups window.

Modify a Device Group

1. In the Device Groups window, select the name of the group you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields. The [Clear] button clears all field values.
4. Click [OK] to save the changes, or on the [Cancel] button to revert to the previously saved values.

Delete a Device Group

1. In the Device Groups window, select the name of the group you wish to delete.
2. Click [Delete].

3. Click [OK].
4. Click [Yes] to confirm.

CHAPTER 37

Local I/O Folder

The Local I/O folder contains forms with which you can:

- Create local I/O function lists, each consisting of a sequence of actions to be performed, such as changing reader modes, activating outputs, and opening or closing anti-passback areas
- Link events to local I/O function lists such that a particular event occurring at a particular device will execute the function list

The folder contains two forms, the Local I/O Function Lists form and the Device-->Function Links form.

The Local I/O folder is displayed by selecting ***Local I/O*** from the ***Access Control*** menu, or by selecting the Local I/O toolbar button.

Toolbar Shortcut

Hardware Dependencies

Although basically the same Local I/O interface is available for all hardware types, there are some hardware-dependent differences for Lenel panels:

- Lenel hardware has a simple interface which will always cause a function list to be executed when triggered by an event link
- Lenel hardware will always log an event when a function list is executed
- The available functions may differ slightly

NGP Limitations

The following are limitations for Local IO when using an NGP Access Panel:

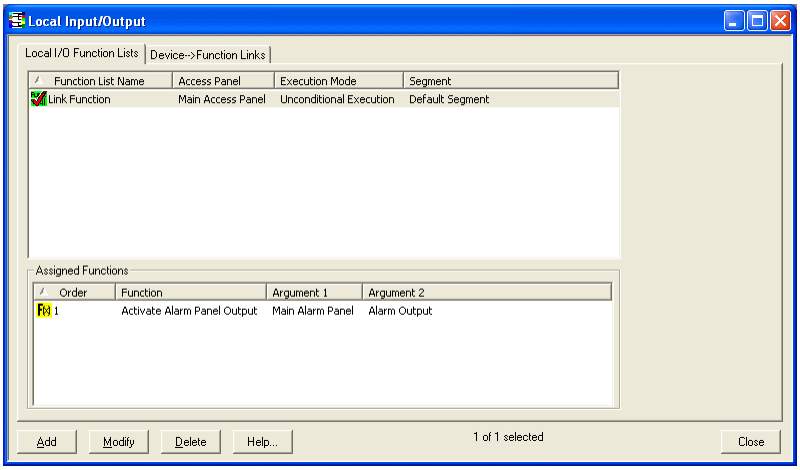
- NGP only supports three functions.
- There is no display or execution from Alarm Monitoring

- The Global action “Execute Function List” does not work for NGP.

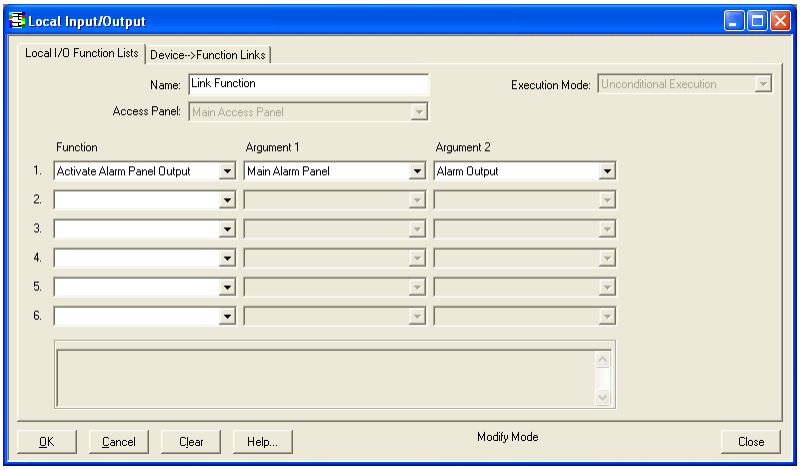
Local I/O Function Lists Form

This form is used to create local I/O function lists, each consisting of a sequence of actions to be performed, such as changing reader modes, activating outputs, and opening or closing anti-passback areas. A typical use of a function list is to trigger a series of outputs.

Local I/O Function Lists Form (View Mode)



Local I/O Function Lists Form (Modify Mode)



Listing window

(displayed in view mode only) Lists all currently defined local I/O function lists, the access panel associated with each, and the execution mode for each.

Assigned Functions

(displayed in view mode only) Lists the functions contained in the selected local I/O function list.

Each function entry indicates the function’s number in the execution sequence, the name of the function, and the values of up to two arguments for the function.

Name

(displayed in modify mode only) Indicates the name of the local I/O function list.

Execution Mode

(displayed in modify mode only) Indicate the circumstances under which the system will execute the function list. Choose one of the following:

- Execute on State Change - indicates that the function list will execute when the state of the list changes from True to False, or from False to True (this not is enabled only for Lenel panels)
- Unconditional Execution - indicates that the function list will always execute

Function (continued)

(displayed in modify mode only) Specify the functions contained in the local I/O function list. A function list can contain up to six functions, some of which may have one or two modifiers called *arguments*. The same function can be included more than once in a list, but typically with different arguments each time. If you require more than six functions in a list, you can link multiple function lists such that they will execute in sequence.

Function 1 (continued)

For each function field you can choose one of the following. Note that when you select a function, relevant information about it is displayed in the **Function Behavior** field at the bottom of the form.

Activate Alarm Panel Output - indicates that the specified alarm panel output will be triggered. This function has two arguments. Available for use with the NGP panel.

- Argument 1 - the alarm panel. Choices include all alarm panels connected to the selected **Access Panel**. Alarm panels are defined on the Alarm Panels form of the Alarm Panels folder.
- Argument 2 - the output to be activated. Choices include all outputs of the alarm panel selected for Argument 1. Outputs are named on the Alarm Outputs form of the Alarm Panels folder.

Function 2 (continued)

Activate Reader Output - indicates that the specified reader output will be triggered. This function has two arguments.

- Argument 1 - the reader. Choices include all readers connected to the selected **Access Panel**. Readers are defined on the Reader form of the Readers folder.
- Argument 2 - the output to be activated. Choices include all outputs of the reader selected for Argument 1. Outputs are named on the Aux Inputs/Outputs form of the Readers folder.

Function 3 (continued)

Alarm Group Mask/Unmask - indicates that the specified group of alarms will be either masked or unmasked. This function has one argument.

- Argument 1 - the alarm mask group, which contains specific devices and alarms. Choices include all currently defined alarm mask groups that are associated with the selected **Access Panel**. Alarm Mask Groups are defined on the Alarm Mask Groups form of the Groups folder.

Function 4 (continued)

Area Open/Close - indicates that the specified anti-passback area will be either opened or closed. This function has one argument. Available for use with the NGP panel.

– Argument 1 - the area to be opened or closed. Choices include all currently defined areas. Areas are defined on the Anti-Passback Areas form of the Areas folder.

Notes: When Area Open/Close is used in a function list on supported panels:

If you set the area to True (open) and the area is already open, the input argument will be set to “Do Nothing”. This means that all subsequent functions in the function list will be set to “Do Nothing”. The same applies if you set the area to False (close) and the area is already closed.

If you set the area to Pulse (open/close), the input argument is changed to True if the new state is open, and False if the new state is closed. Since this function changes the input argument, the behavior of subsequent functions in the list may be affected.

When Area Open/Close is used in a function list on a Lenel panel:

True sets the area to open, False sets the area to closed, and Pulse does nothing.

Function 5 (continued)

Chain to Function List – calls another function list. It is used to link two or more lists in situations that require more than six functions. It is for this reason that the function is typically placed at the end of the function list. This function has one argument.

– Argument 1 - the local I/O function list to be linked to the current one. Choices include all currently defined local I/O function lists, as defined on this form. BE VERY CAREFUL NOT TO RECURSIVELY LINK TWO LOCAL I/O FUNCTION LISTS (i.e., have a list call a second list, which then calls the first list), AS THIS WILL PUT THE SOFTWARE IN AN INFINITELOOP.

Function 6 (continued)

Log Event - generates an event indicating that this function list was executed. It is typically the last function in the list. This function has no arguments. Note that this function is not available for LNL-1000 access panels.

Function 7 (continued)

Dialback to Host - dials the modem attached to the host computer. This function has no arguments. It is used for event reporting in environments where the access panel is linked to a remote host computer via modem. The function list can be linked to any action that can occur on the panel. Note that this function is available only for LNL-1000 access panels.

When the function list is executed, the panel will attempt to dial the host (your application server). After the panel’s transactions are dumped and any necessary commands are sent from the host to the panel, the host will terminate the connection.

For example, suppose that you have a reader named “Vault Reader” connected to a vault door. Using this form, you create a function list called “Call Headquarters” that includes the “Dialback to Host” function. Using the Device Function Links form, you link “Vault Reader” to the “Call Headquarters” function list and the “Door Forced Open” event. Then, if someone forces the vault door open, the application will dial the phone number of the modem on the remote host computer and report a “Door Forced Open” alarm.

Function 8 (continued)

Reader Unlock/Set Mode - Changes the mode of the selected reader to Unlocked when executed with TRUE, and back to the selected mode when executed with FALSE. This function has two arguments. Available for use with the NGP panel.

– Argument 1 - the reader. Choices include all readers connected to the selected **Access Panel**. Readers are defined on the Reader form of the Readers folder.

- Argument 2 - the reader mode to revert back to. Choices include Card and PIN, Card only, Facility Code only, Locked, PIN or Card, and Unlocked.

Function 9 (continued)

Test for Active Alarms in Alarm Group - checks the status of the specified alarm mask group. This function has one argument.

- Argument 1 - the alarm mask group, which contains specific devices and alarms. Choices include all currently defined alarm mask groups that are associated with the selected **Access Panel**. Alarm Mask Groups are defined on the Alarm Mask Groups form of the Groups folder.

Note: If you set this function to false and if any of the alarms in the specified alarm mask group are active, the input argument will be set to "Do Nothing". This means that all subsequent functions in the function list will be set to "Do Nothing".

Function 10 (continued)

Timezone Activate/Deactivate - activates or deactivates the selected timezone. The selected timezone will remain in that state until the next interval. This function has one argument.

- Argument 1 - the timezone to be activated or deactivated until the next interval. Choices include all currently defined timezones. Timezones are defined on the Timezones form of the Timezones folder.

Function 11 (continued)

Timezone Override - activates or deactivates the selected timezone permanently. The selected timezone will remain in that state until an activation or deactivation command is issued. This function has one argument.

- Argument 1 - the timezone to be activated or deactivated permanently. Choices include all currently defined timezones. Timezones are defined on the Timezones form of the Timezones folder.

Function 12 (continued)

Area Force Arm/Disarm - indicates the specified area will be armed or disarmed. As a Forced Arm command, automatically bypasses any points (zones) currently in active/trouble states to allow arming. Available for use with the NGP intrusion panels (NGP-2220i and NGP-3320i). This function has one argument.

- Argument 1 - the area to be armed or disarmed. Choices include all areas currently associated with the selected access panel. Areas are defined on the Areas form of the Areas folder.

Function 13 (continued)

Area Force Stay/Disarm - indicates the specified area will be stay armed or disarmed. Stay Arm will arm only the designated interior protection points (for example, motion sensors and interior doors). Available for use with the NGP intrusion panels (NGP-2220i and NGP-3320i). This function has one argument.

- Argument 1 - the area to be stay armed or disarmed. Choices include all areas currently associated with the selected access panel. Areas are defined on the Areas form of the Areas folder.

Argument 1

(displayed in modify mode only) A modifier that is applied to the current function. It provides required, detailed information for the function. For example, the function "Alarm Group Mask/

Unmask" may have the argument "Main Lobby", which tells the system to mask or unmask alarms specified by the Main Lobby alarm mask group.

Argument 2
(displayed in modify mode only) If a function requires two arguments, this field is used to select the second one.

Function Behavior
(displayed in modify mode only) Provides descriptive information about the selected function.

Add
Used to add a local I/O function list.

Modify
Used to change a local I/O function list.

Delete
Used to delete a local I/O function list.

Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as "1 of 42 selected"). In modify mode, indicates the current operation, such as "Modify Mode."

Close
Closes the Local I/O folder.

Access Panel
(displayed in modify mode only) The access panel on which the function list operates.

Local I/O Function Lists Form Procedures

Use the following procedures on this form.

Add a Local I/O Function List

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for the list.
3. Select an access panel from the **Access Panel** drop-down list.
4. Select an execution mode from the **Execution Mode** drop-down list. The execution mode describes the circumstances under which the system will execute the function list. Choices include:
   - Execute on State Change - indicates that the function list will execute when the state of the list changes from True to False, or from False to True (this not is enabled for Lenel panels)
   - Unconditional Execution - indicates that the function list will always execute
5. For each function statement you want to include in the list:

a. Select the function name from the **Function** drop-down list. Notice that the **Function Behavior** display box is updated with descriptive information about the selected function.
b. If the function requires an argument, select its value from the **Argument 1** drop-down list.
c. If the **Argument 2** field is activated, select the second argument from that drop-down list.

6. Click [OK].

Note: If you want to include more than six function statements in the list, create a second function list for that Access Panel. Then you can modify the first list to select **Chain to Function List** for the sixth function.

Modify a Local I/O Function List

1. In the listing window, select the local I/O function list you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Make the changes you want to the fields. The [Clear] button clears all field values.

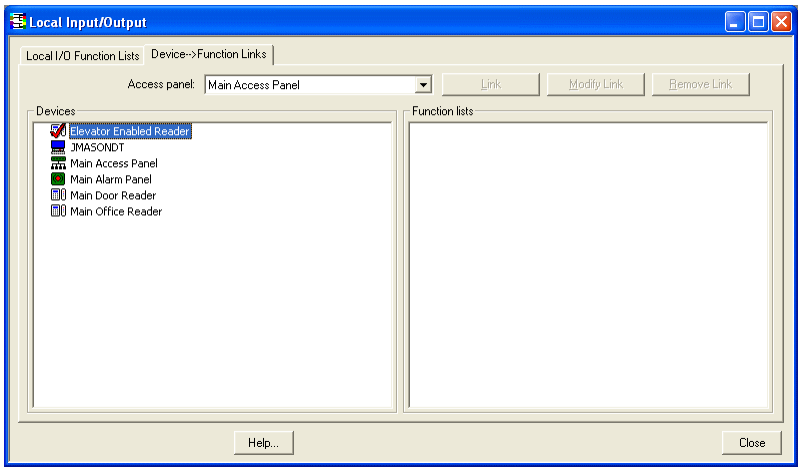
   Note that you can't change the **Access Panel** selection, because all other selections depend upon it.
5. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Local I/O Function List

1. In the listing window, select the local I/O function list you wish to delete.
2. Click [Delete].
3. Click [OK].
4. Click [Yes] to confirm.

Device --> Function Links Form

This form is used to link events to local I/O function lists such that a particular event occurring at a particular device will execute the function list.



Access Panel
The access panel whose devices and function list you wish to link.

Devices
Lists all linkable devices that are connected to the selected access panel. An icon precedes the access panel entry. An icon precedes each alarm panel entry. An icon precedes each reader entry. An icon precedes the entry for the workstation to which the access panel is attached. An icon precedes the entry for the area associated with the NGP access panel. Subentries preceded by a ↳ indicate links between devices and function lists. These links are also listed in the Function Lists window.

Function Lists
Lists all local I/O function lists associated with the selected access panel. Subentries preceded by a ↰ indicate links between devices and function lists. These links are also listed in the Devices window.

Link
Used to link a device and a function list.

Modify Link
Changes the state/action parameters for a device-to-function list link.

Remove Link
Removes the link between a device and a function list.

Close
Closes the Local I/O folder.

Device --> Function Links Form Procedures

Use the following procedures on this form.

Link A Device to a Local I/O Function List

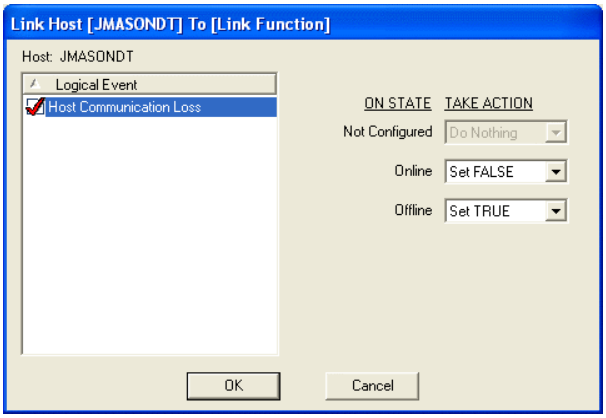
1. Select an access panel from the **Access Panel** drop-down list.
   - Hardware associated with the selected **Access Panel** will be listed in the **Devices** field. This includes the access panel, readers, alarm panels, and workstation.
   - Local I/O function lists associated with the selected **Access Panel** will be listed in the **Function Lists** field. Note: you cannot create a link unless at least one function list has been created for the panel.
2. Select an item in the Devices list.
3. Select a local I/O function list in the **Function Lists** field. Note that the [Link] button is activated.
4. Click [Link].
5. A Link window will be displayed. The contents of the Link window vary with the device type and also with the Logical Event selected in the Link window itself. Refer to the following sections for an illustration of each window type:

- Link Host Form on page 799
- Link Access Panel Form on page 799
- Link Alarm Panel Form on page 800
- Link Reader Form on page 801
- Link Area Form on page 803

6. In the Link window, choose a **Logical Event** from the list. The State/Action parameters will be displayed.
7. For each item in the On State list, select the corresponding **Take Action** choice. The choices are:
   - Do Nothing - when the event is in that state, does nothing to the specified term of the specified function list. Typically, for a “Not Configured” state, you would choose this action.
   - Set TRUE - execute the function list with an input argument of TRUE
   - Set FALSE - execute the function list with an input argument of FALSE
   - PULSE - execute the function list with an input argument of PULSE
8. Click [OK].

Link Host Form

This view is displayed when linking a workstation with an access panel attached to it to a function list.



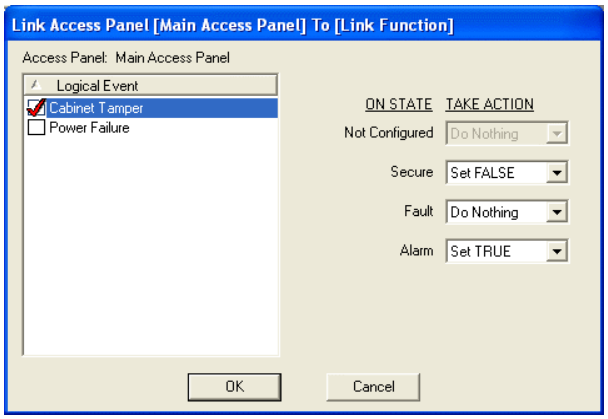
Not Configured
The access panel is not configured on the host (workstation)

Online
The access panel is online and communicating properly with the host

Offline
The access panel is offline to the host

Link Access Panel Form

This view is displayed when linking an access panel to a function list.



Not Configured
The access panel is not configured on the host

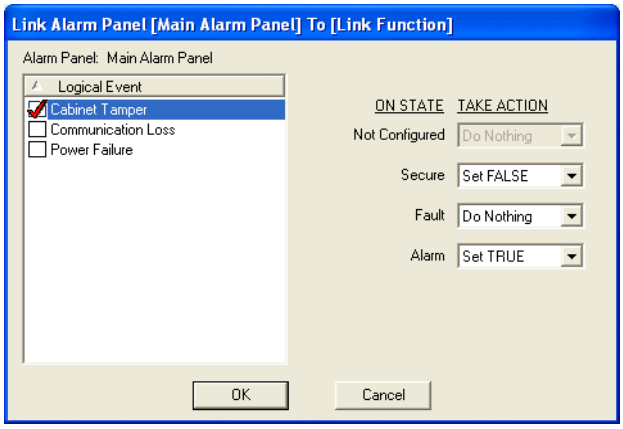
Secure
The access panel is operating normally

Fault
The access panel is experiencing a trouble condition

Alarm
The access panel is in an abnormal state

Link Alarm Panel Form

This view is displayed when linking an alarm panel to a function list and either the Cabinet Tamper or Power Failure logical event is selected.



Not Configured
The alarm panel is offline. If the selected logical event is an input, the input is considered to be "Not Configured" if it's configured as "offline".

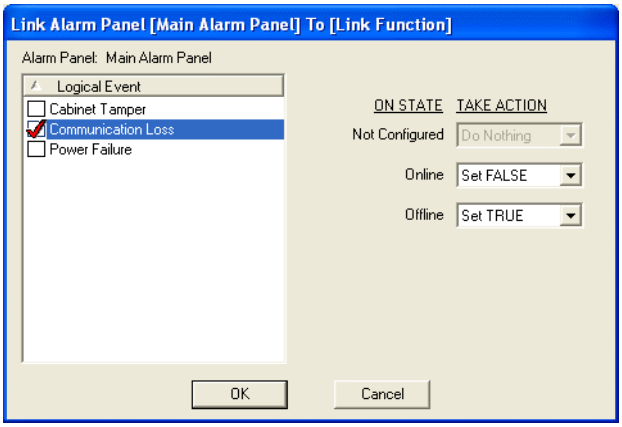
Secure
The alarm panel is operating normally

Fault

The alarm panel is experiencing a trouble condition

Alarm

The alarm panel is in an abnormal state. This view is displayed when linking an alarm panel to a function list and the Communication Loss logical event is selected.



Not Configured

The alarm panel is not configured on the host (workstation)

Online

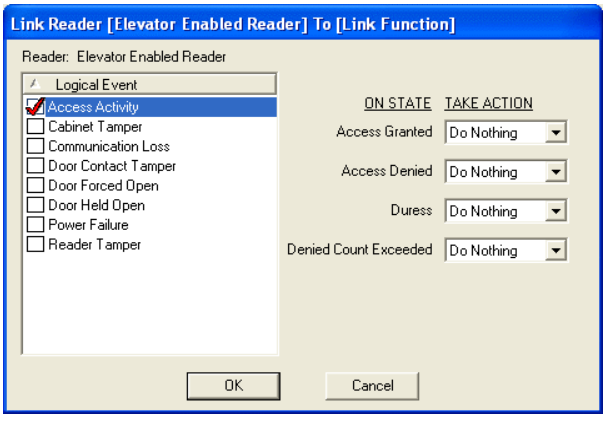
The alarm panel IS communicating to the host

Offline

The alarm panel IS NOT communicating to the host

Link Reader Form

This view is displayed when linking a reader to a function list and the Access Activity logical event is selected.



Access Granted

An Access Granted alarm has occurred at the reader

Access Denied

An Access Denied alarm has occurred at the reader

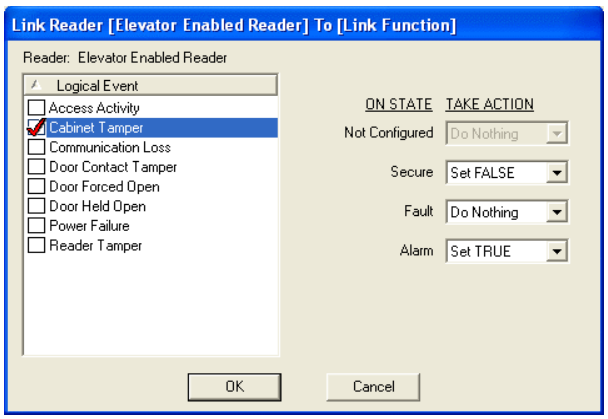
Duress

A Duress alarm has occurred at the reader

Denied Count Exceeded

The **Denied Attempts Count** (“also called “Diddle Count”) value has been exceeded This field only appears if the **Count** field in the Denied Attempts section on the Settings tab for the reader is set to a value greater than 0.

This view is displayed when linking a reader to a function list and the Cabinet Tamper, Door Contact Tamper, Door Forced Open, Door Held Open, Power Failure, or Reader Tamper logical event is selected.



Not Configured

The reader is not configured on the host

Secure

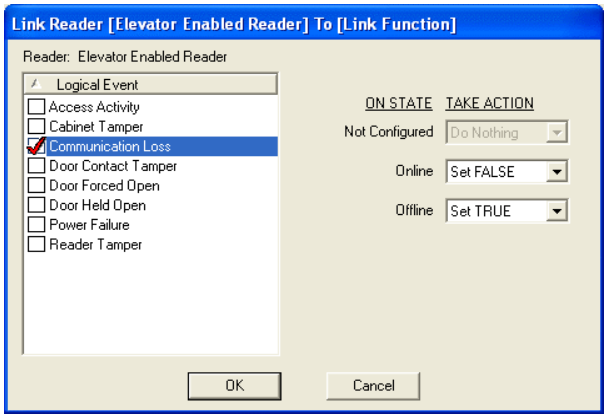
The reader is operating normally

Fault

Fluctuating resistance has resulted in a fault in the reader or in its communication to the panel

Alarm

An alarm has been triggered by this reader. This view is displayed when linking a reader to a function list and the Communication Loss logical event is selected.



Not Configured

The reader is functioning properly and is communicating to the access panel, but the access panel isn't detecting the reader.

Online

The reader is functioning and is communicating properly with the access panel.

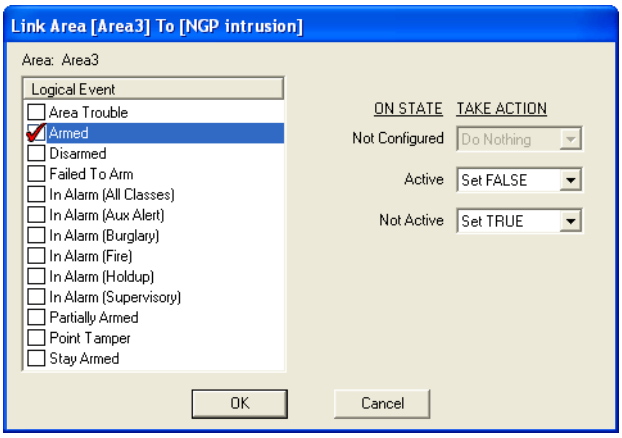
Offline

The reader is NOT communicating with the access panel.

Link Area Form

Note: This functionality is available for NGP intrusion access panels, NGP-2220i and NGP-3320i, only.

This view is displayed when linking an area associated with an NGP intrusion panel to a function list and the Armed logical event is selected.



Not Configured

The access panel is offline. If the selected logical event is an output, the output is considered to be "Not Configured" if it is configured as "offline."

Active

The area armed state is active.

Not Active

The area armed state is not active.

CHAPTER 38

Global I/O Folder

The Global I/O folder contains the Global Linkage form with which you can:

- Link any input event a controller is aware of to any output action a controller may cause in the same region
- Define Global I/O linkage lists that span controllers

This folder is displayed by selecting ***Global I/O*** from the ***Access Control*** menu, or by selecting the Global I/O toolbar button.

Toolbar Shortcut

Global I/O Overview

The Global I/O feature from previous versions has been renamed Local I/O. What is the difference between Local I/O and the new, expanded Global I/O? Both allow input events to be linked to output actions. The difference is that for Local I/O, the input event and the output action must use the same controller, whereas for Global I/O, the input event can initiate an output action on any other controller that is in the same region.

Note: An access panel is a type of controller.

The following table compares the features of Local I/O and Global I/O:

Feature	Local I/O	Global I/O
Events are viewable in Alarm Monitoring and are subject to alarm filtering	X	X
Input events can be linked to output actions using a single controller	X	X

Feature	Local I/O	Global I/O
Input events can be linked to output actions using multiple controllers in the same region		X
A timeout period can be specified for a linkage which indicates how long after an input is activated it will remain valid and can cause an output action		X
Failed linkages are displayed in Alarm Monitoring and are subject to alarm filtering		X
Failed linkages are logged		X
A linkage can be executed during a specified access control timezone and World Time Zone		X
Specific user's card access activity (i.e., badge number) can be used as an input event		X

User Permissions for Global I/O

Each form/feature requires certain permissions in an access control system user's profile in order for them to be able to access the Global I/O features. User permissions for Global I/O consist of being able to view, add, modify, or delete Global I/O linkages. Global I/O permissions are set on the System Permission Groups form in the Users folder (in the System Administration and ID CredentialCenter applications).

Global I/O and Alarm Monitoring

You can use Alarm Monitoring to view Global I/O linkage activity.

- When an input event is received that is configured to cause an output action, the linkage that was performed is displayed in Alarm Monitoring and is subject to alarm filtering.
- If the output action of a Global I/O linkage cannot be initiated, the notification will be displayed as an alarm in Alarm Monitoring. This alarm is subject to alarm filtering, and is logged.

Global I/O and Segmentation

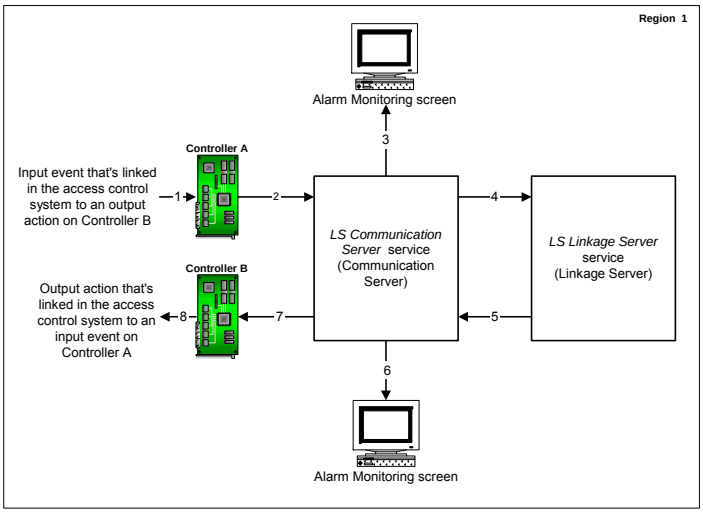
Global I/O linkages can belong to a segment, segment group, or to all segments. In a segmented system, you will be prompted with the available segments and segment groups that you have access to for the Global I/O linkage. The following applies to segmented systems:

- To modify or delete a Global I/O linkage, a user must have access to all segments the linkage belongs to.
- To view a Global I/O linkage, a user only needs to have access to one segment that the linkage belongs to. Although all items are listed, only those in the user's segment will be fully displayed.
- When an input event is configured, only the hardware in the segment(s) for that Global I/O linkage will be displayed.
- When configuring output actions, only those actions that belong to the same segment(s) as the Global I/O linkage will be available.

How Do Global I/O Linkages Work?

The following diagram describes what happens when an input event on Controller A causes an output action on Controller B when a Global I/O linkage has been set up in the access control software. Controller A and Controller B must be in the same region.

Global I/O Process Flow



The numbers below describe the process that occurs at each of the numbers in the diagram above.

1. An input event is defined as part of a Global I/O linkage in the access control software, and has an output action on Controller B assigned to it. The input event occurs on Controller A.
2. The Communication Server receives the input event.

Steps 3 and 4 occur at virtually the same time.

3. The Communication Server sends notice of the input event to Alarm Monitoring. The input event is filtered and displayed on the Alarm Monitoring screen.
4. The Linkage Server "listens" to events received by the Communication Server. The Linkage Server distinguishes the Global I/O input event from all others.
5. Based on the input event, the Linkage Server tells the Communication Server the appropriate Global I/O output linkage that needs to be executed.

Steps 6 and 7 occur at virtually the same time.

6. The Communication Server sends notice of the output action to Alarm Monitoring. The output action is filtered and displayed on the Alarm Monitoring screen.
7. The Communication Server communicates the action output to Controller B.
8. Controller B performs the action output.

What if a Global I/O Linkage Fails?

There are two main reasons why a Global I/O linkage might fail: if the input-event controller is offline, or if the output-event controller is offline.

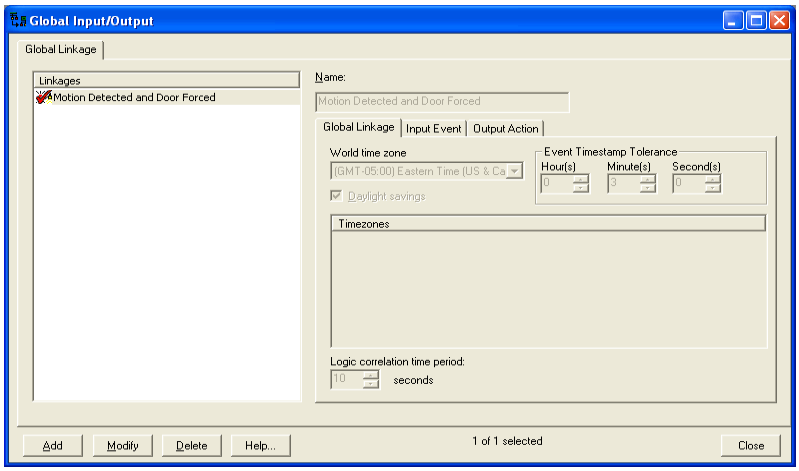
- If a controller generates an input event but can't communicate with it's host, the input event will not be detected by the host, and the linkage will not be carried out at least until the controller and host communication is re-established. If the connection is re-established, the settings in the Event Timestamp Tolerance section on the Global Linkage sub-tab of the Global Linkage form will determine whether or not the output action is initiated.

- If a controller generating an output action cannot communicate with it's host, the output action to be carried out cannot be sent to the output-generating controller and the linkage will not be carried out. The failed output action will be logged.

Global I/O Considerations

If the communication servers are run on different machines than the Linkage Server then you should keep the time of the machine running the Linkage Server accurate to the closest possible second. If the times are not in sync between machines then problems may occur in Global I/O linkage executions.

Global Linkage Form (Global Linkage Sub-tab)



Linkages listing window

Lists currently defined Global I/O linkages and the segment each is associated with (if segmentation is enabled).

Name

Specifies a name for this Global I/O linkage. You can enter a name containing a maximum of 32 characters.

Add

Used to add a Global I/O linkage entry.

Modify

Used to change a Global I/O linkage entry.

Delete

Used to remove a Global I/O linkage entry.

Help

Displays online help for this form.

Close

Closes the Global I/O folder.

World Time Zone

Select the world time zone for the selected Global I/O linkage's geographical location. The default world time zone is the world time zone on the computer that the linkage is being configured on.

A Global I/O linkage can be configured to occur only during a selected access control timezone in a selected world time zone. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Event Timestamp Tolerance

Contains the **Hour(s)**, **Minute(s)**, and **Second(s)** fields. If you set the Event Timestamp Tolerance to 0 (by entering 0 into the **Hour(s)**, **Minute(s)**, and **Second(s)** fields), the global I/O linkage will execute regardless of how old the event is. Basically, when you set the Event Timestamp Tolerance to 0, it is not used.

Hour(s)

Number of hours that an input event remains valid after it has been generated and may cause a linkage to take place. Used in conjunction with the **Minute(s)** and **Second(s)** fields.

Minute(s)

Number of minutes, in addition to the number of hours, that an input event remains valid after it has been generated and may cause a linkage to take place.

Second(s)

Number of seconds, in addition to the number of hours and minutes, that an input event remains valid after it has been generated and may cause a linkage to take place.

Daylight savings

Select this check box if daylight savings time is used in the selected world time zone.

Timezones listing window

Indicates the range of time that a linkage is valid for. Timezones are added on the Timezones form, which is displayed by selecting the ***Access Control*** **>** ***Timezones*** menu option and then clicking the Timezones tab.

Logic correlation time period

When creating a linked alarm event, set this to the number of seconds that must occur between each event for the events to be valid. This is a rolling time limit where the time period resets after each correlating event occurs.

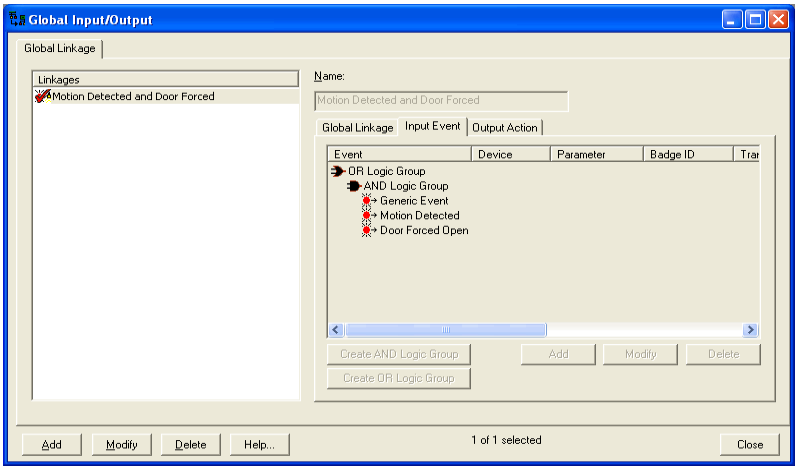
Global Linkage Form (Input Event Sub-tab)

Input events are events that are detectable by the Linkage Server and may cause a Global I/O linkage to occur. The following examples are a few of the input events:

- Any predefined OnGuard event
- A user access event for a specific badge. This can be configured based on either of the following:
  - An event and badge number

  - An event, badge number, and hardware device
- An event and hardware device
- An event, hardware device, and badge device

Note: Since Global I/O compares the time of incoming events with the time on the Linkage Server machine time synchronization becomes important. If the communication servers are run on different machines than the linkage server then you should keep the time of the machine running the Linkage Server accurate to the closest possible second. If the times are not in sync between machines then problems may occur in Global I/O linkage executions.



Input event listing window

Displays the event, device, parameter, badge ID, transmitter, transmitter input, and event for each input event that is associated with the selected Global I/O linkage. There may be multiple input events associated with a single event.

Create AND Logic Group

With two or more events selected you can click this button to group the selected events together into a logic group. The multiple events must occur within a set amount of time as defined by the **Logic correlation time period** found on the Global Linkage Sub-tab to be considered grouped together.

Create OR Logic Group

After creating an AND logic group you are able to modify it by adding an OR logic group. After selecting events in the AND logic group click this button to create an OR subset of the AND logic group. How this works is that the events listed in the AND logic group and one or the other of the OR logic group events must occur for the alarm to appear in Alarm Monitoring.

Add

This button is used to add an input event for the selected Global I/O linkage. It is enabled for selection only when the Global Linkage form is in Add or Modify mode.

Modify

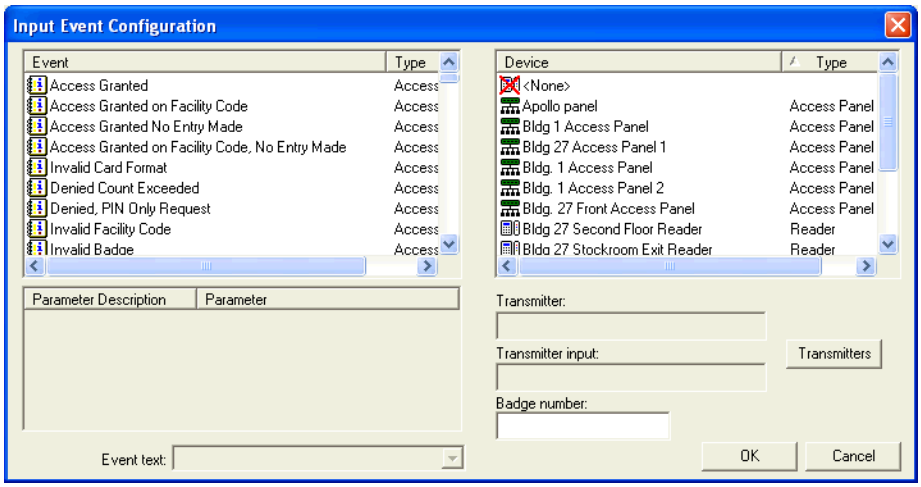
This button is used to modify an input event for the selected Global I/O linkage. It is enabled for selection only when the Global Linkage form is in Modify mode and an input event is selected.

Delete

This button is used to delete an input event from the selected Global I/O linkage. It is enabled for selection only when the Global Linkage form is in Modify mode and an input event is selected.

Input Event Configuration Form

This form is displayed when the [Add] button on the Input Event sub-tab is clicked.



Event listing window

Shows the list of events that may initiate a linkage, including the event description and the type of event. When configuring an input event, an event must be selected.

Parameter Description

If the event selected in the Event listing window can have parameters, they are listed here.

Device listing window

Selecting a device is optional. All devices the current user may view as well as the type of device that is being viewed are displayed.

Event text

This field works in conjunction with generic events. Use this field when you send multiple events under the Generic event category and you want to identify a specific event that will trigger an output.

For example, you may have an OPC Source that sends “Alarm Active” and “Alarm Restored” under the Generic event category. By entering specific event text, you can control what generic event triggers an output. In the example mentioned above, if you enter “Alarm Active” in the Event text field, the Global I/O linkage executes the output when that generic event comes in and not when the “Alarm Restored” generic event comes in.

You can either enter event text or select text created in the Text Library form, which is located by selecting ***Text Library*** from the ***Administration*** menu.

Transmitter

Displays the name of the transmitter selected in the Input Event Transmitter Configuration window (displayed by selecting the [Transmitters] button).

Transmitter input

Displays the name of the transmitter input selected in the Input Event Transmitter Configuration window (displayed by selecting the [Transmitters] button).

Transmitters

Click this button to display the Input Event Transmitter Configuration window from where you can select the transmitter and optionally a transmitter input.

This button is enabled only if you have a license for devices that can support transmitters.

Badge Number

Selecting a badge number is optional. If a badge number is specified, the output action will only be initiated when the input event occurs for that badge number.

OK

Saves selections or changes and returns you to the Input Event sub-tab.

Cancel

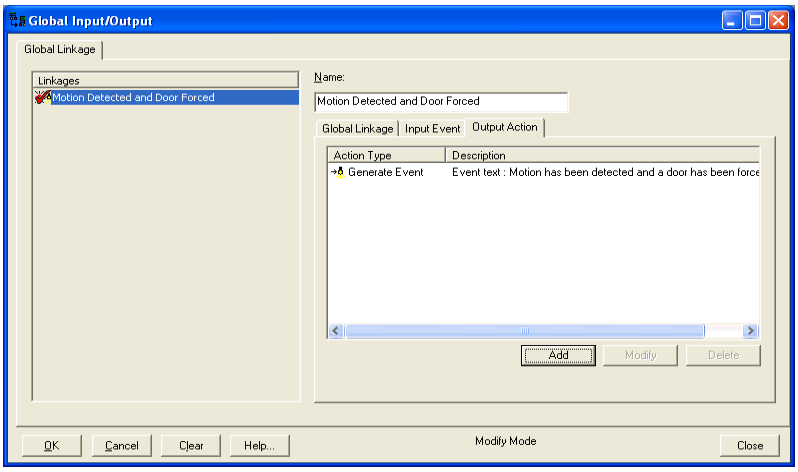
Cancels pending selections or changes and returns you to the Input Event sub-tab.

Global Linkage Form (Output Action Sub-tab)

Output actions are actions that may be performed as the result of a Global I/O linkage. The following can be output actions:

- Action Group
- Arm/Disarm Area
- Change Network Video Password
- Deactivate Badge
- Device Output
- Device Output Group
- Elevator Terminal Allowed Floors
- Elevator Terminal Mode
- Execute Function List
- Generate Event
- Grant/Deny Popup
- Intercom Call
- Mask/Unmask Alarm Input
- Mask/Alarm Input for Group
- Mask/Unmask Alarm Mask Group
- Mask/Unmask Door
- Mask/Unmask Door Forced Open
- Mask/Unmask Door Forced Open for Reader Group
- Moving Badges for APB Areas
- Muster Mode Initiation
- Open/Close APB Area
- Pulse Open Door

- Pulse Open Door Group
- Reader Mode
- Reader Mode Group
- Report Print
- Reset Use LImit
- Run PTZ Tour
- Select PTZ Preset
- Select Video Wall Layout
- Sign Out Visitor
- Silence Area



Output action listing window

Displays the action type and description for each output action that is associated with the selected Global I/O linkage.

Add

This button is used to add an output action for the selected Global I/O linkage. It is enabled for selection only when the Global Linkage form is in Add or Modify mode.

Modify

This button is used to modify an output action for the selected Global I/O linkage. It is enabled for selection only when the Global Linkage form is in Modify mode and an output action is selected.

Delete

This button is used to delete an output action for the selected Global I/O linkage. It is enabled for selection only when the Global Linkage form is in Modify mode and an output action is selected.

Global Linkage Form Procedures

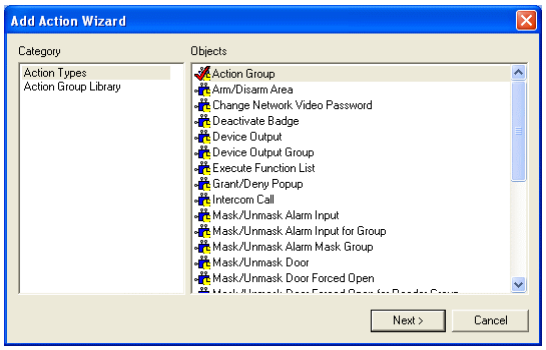
Use the following procedures on this form.

Add a Global I/O Linkage

1. Display the Global Linkage folder and click [Add].
2. If segmentation is enabled:
   a. The Segment Membership window opens. Select the appropriate segment.
   b. Click [OK].
3. In the **Name** field, enter a unique, descriptive name for the Global I/O linkage.
4. On the Global Linkage sub-tab:
   a. Select the World Time Zone during which the Global I/O linkage will function.
   b. Select how long the input event will occur.
   c. If the world time zone you selected uses daylight savings, click the **Daylight savings** check box.
   d. In the Timezones listing window, select the access control timezone during which the Global I/O linkage will function.
5. On the Input Event sub-tab:
   a. Click [Add] to display the Input Event Configuration form.
   b. Select the event that you wish to link.
   c. If you selected "Generic Event," enter the event text in the **Event text** field that will appear when the output executes.
   d. If the event you selected has parameters, select one of the following from the Parameter Description listing window.
      - (Optional) Select the Device.
      - (Optional) Click [Transmitters] to display the Input Event Transmitter Configuration window. Select a transmitter and a transmitter input.
      - (Optional) Select a Badge Number.

Note: You cannot select both a transmitter and a badge at the same time. You must use one or the other.

   e. Click [OK].
   f. Repeat steps a–e for every input event linkage you wish to add.
   g. Optionally you can add event correlation. For more information, refer to Global I/O Event Correlation on page 816.
6. On the Output Action sub-tab:
   a. Click [Add]. The Add Action Wizard window opens.



   - If you select "Action Types," a list of output actions which may be associated with a linkage displays.

- If you select “Action Group Library,” entries in the Action Group Library display and may be associated with a linkage.

For more information please refer to Appendix A: Actions on page 1193.

b. Repeat step a for every output action linkage you wish to add.

7. Click [OK].

Modify a Global I/O Linkage

1. In the Linkages listing window, select (click on) the name of the Global I/O linkage you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields. Changes can be made on any sub-tab. To modify an input event:
   a. Click the Input Event sub-tab.
   b. Select the input event you want to modify.
   c. Click [Modify]. The Input Event Configuration window will be displayed. Make the changes you want to make.
   d. Click [OK].

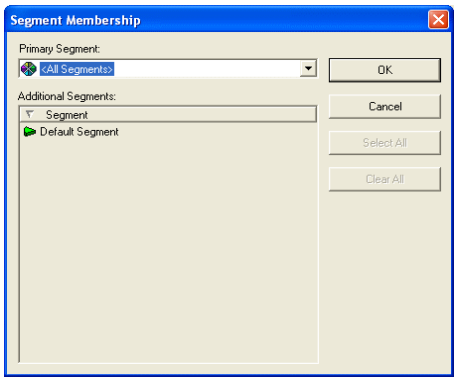
   To modify an output action:
   e. Click the Output Action sub-tab.
   f. Select the output action you want to modify.
   g. Click [Modify].
   h. The properties window for the selected output action will open. For more information please refer to Appendix A: Actions on page 1193.
   i. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Global I/O Linkage

1. In the Linkages listing window, select (click on) the name of the Global I/O linkage.
2. Click [Delete].
3. Click [OK].
4. Click [Yes] to confirm the deletion.

Modify a Global I/O Linkage’s Segment

1. In the Linkages listing window, select (click on) the name of the Global I/O linkage you wish to change.
2. Click [Modify].
3. Click [Change Segment]. The Segment Membership window opens.
4. Select a segment to move the Global I/O linkage to.



5. Click [OK].
6. If segmentation is not enabled, skip this step. If segmentation is enabled, the timezones are updated to show only the timezones in the segment that you just changed the Global I/O linkage to. You must select a new timezone, which is done on the Global Linkage sub-tab in the Timezones listing window.
7. Click [OK].

Global I/O Event Correlation

Event correlation, at its base, restricts output based on user-defined correlations between input events. One outcome of this is that you can create a custom alarm to be generated when two or more events, based on certain logic conditions, occur within a set time period.For example, you may want a custom alarm to be reported if the “Motion Detected and “Door Forced Open” events occur within a certain number of seconds of each other. Linking these two events together creates a new alarm that is generated in Alarm Monitoring when these two events occur and an output action has been created for it.

The timing used to see whether the events are linked is determined by the timestamp provided by the hardware you are using. Because of this it is vitally important that all of your hardware is synced to have the same time.

Adding a Global I/O Event Correlation

1. Make sure that the events you wish to link are already added. For more information, refer to Add a Global I/O Linkage on page 814.
2. To link the events, first click [Modify].
3. On the Input Event sub-tab, select two or more events on the Input Event sub-tab and click **Create AND Logic Group**. This will link the events together under the AND Logic Group title. In the listing window you will see this represented as a listing tree. When creating an AND Logic Group the topmost item in the tree will be an empty OR Logic Group heading. You may add events here which act as independent events from the AND Logic Group. Events can be dragged and dropped to change their position in this listing window.

Note: On the Global Linkage sub-tab, you can change the value of the Logic correlation time period spin-box to the number of seconds that each event will have to occur between one another to be considered linked. This is a rolling time limit where the time period resets after each correlating event occurs.

4. Optionally, you can further customize these linked events by adding an OR Logic Group under the AND Logic Group. Do this by selecting two or more event in the AND Logic Group and clicking **Create OR Logic Group**. This will add another layer of complexity to the event correlation before the output action is executed. Let's walk through a short example:
   a. If you have three events (A,B and C) that have to occur within a certain amount of seconds to be considered linked events you will select all three and click **Create AND Logic Group**.
   b. Now, let's say you also have events D and E but only one or the other has to occur along with events A,B, and C to be considered linked. You would then select events D and E and click **Create OR Logic Group**. This creates a linked event that occurs only when events A,B,C, occur together along with either D or E.
5. On the Output Action sub-tab:
   a. Click [Add]. The Add Action Wizard window opens.
      - Select Generate Event. This event allows you to create custom text that allows you to further customize your linked alarms.

Note: Feel free to select any event that you feel will work. Generate Event is just one option for you to use and is only recommended here because of its option for user-defined event text.

6. Click [OK].
7. Optionally, if you are using custom alarms you can elect to turn the display of the individual alarms, the ones that make up your linked alarm, off. You would do this so only your new linked alarm with your custom text is displayed in Alarm Monitoring. To do this:
   a. In System Administration, click "Monitoring" in the menu bar and select "Alarms".
   b. Find the alarms in the listing window whose display you wish to turn off.
   c. Click [Modify].
   d. Un-check **Display Alarm**.
   e. Click [OK].

CHAPTER 39

EOL Tables Folder

The EOL Tables folder contains the EOL Resistor Tables form with which you can add, modify, and delete custom EOL resistor tables.

This folder is displayed by selecting ***EOL Resistor Configuration*** from the ***Access Control*** menu.

Basic Custom EOL Resistor Tables

You can configure up to four (4) custom resistor tables for Lenel access panels using different EOL resistor input configurations (alarm panel inputs, reader inputs, reader door contact, and reader rex).

You can configure up to four (4) custom (BASIC only) resistor tables for NGP access panels using different input configurations (NGP on-board and NGP universal I/O devices).

If segmentation is enabled, you can configure up to four custom resistor tables per segment.

By default, there are four built-in system tables.

- Default Supervision, Normally Closed
- Default Supervision, Normally Open
- Not Supervised, Normally Closed
- Not Supervised, Normally Open

Note: The Default Supervision EOL resistor values are 1k ohms/1k ohms.

Advanced Custom EOL Resistor Tables

A majority of the time, the basic custom EOL resistor tables are sufficient. If you need to use the advanced custom EOL Resistor table you must consult your local hardware dealer.

Advanced custom EOL resistor tables are not supported for devices connected to either NGP access panels or HID access panels. If you attempt to change a “Basic Custom” EOL table to an “Advanced Custom” type for such readers, a warning message will be displayed.

Resistance Values

Lenel input/output boards measure resistance values differently between an advanced and basic table. The advanced table can be set from 50 to 25k ohms. The basic table can be set from 51 to 12499 ohms.

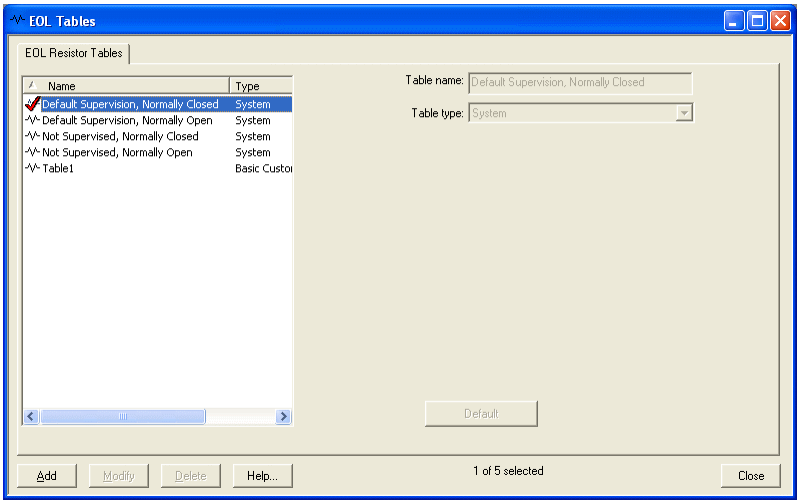
When you enter values for the normal low range, the first field is the resistance value for the inactive state of the circuit. The second field is the resistance value for the active state of the circuit. The same concept applies for the normal high range fields.

You can enter active and inactive values as percentages or absolute values (+/-). Regardless of the method, the lowest value should not be less than 51 ohms (50 on an advanced table) and the highest value should not exceed 12499 (25,000 on an advanced table) ohms. However, each range should be large enough to comfortably cover any noise induced variation.

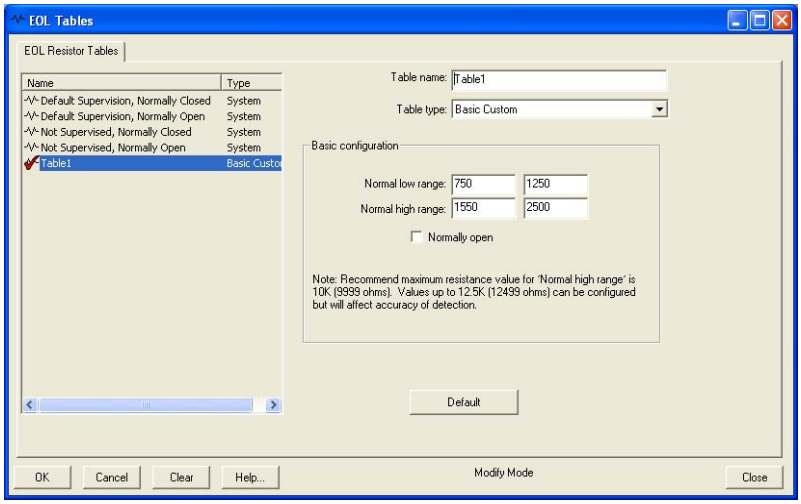
Note: To meet UL 1076 you must detect at least a 50% change in resistance. Resistant measurement is not 100% accurate.

EOL Resistor Tables Form

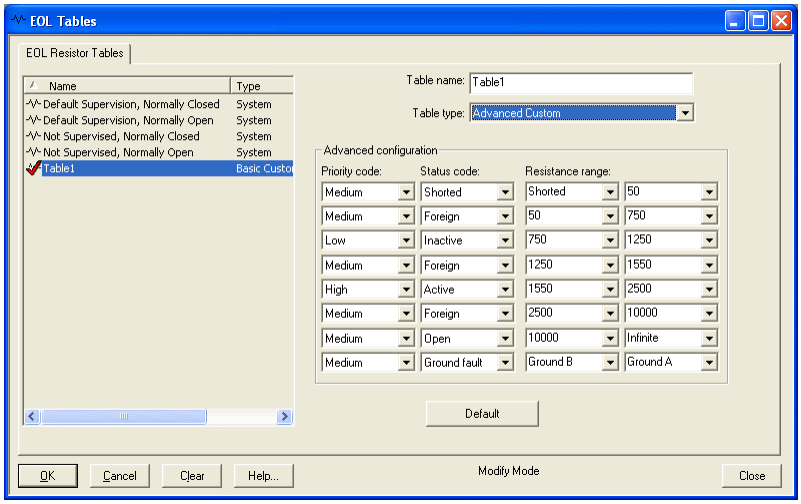
EOL Resistor Tables Form (View Mode)



EOL Resistor Tables Form (basic custom table types)



EOL Resistor Tables Form (basic custom table types)



Listing window

Lists currently defined system and custom EOL resistor tables. An icon precedes each entry.

Table name

Indicates the name for the custom EOL resistor table. The name can contain a maximum of 32 characters.

Table type

Indicates the type of EOL resistor table that is selected in the listing window or that is being configured. Choices in the drop-down list include:

- **Basic Custom** - The basic configuration requires the resistance range for the normal low and normal high ranges to be defined, as well as an indication of whether or not the circuit is normally open. When the **Basic Custom** table type is selected, the **Normal low range**, **Normal high range**, and **Normally open** fields display.
- **Advanced Custom** - There are eight sets of resistance ranges that can be configured. Each range is associated with a priority code and a status code. When the **Advanced Custom** table type is selected, the **Priority code**, **Status code**, and **Resistance range** fields display.

The table type **System** is automatically assigned to the four built-in system tables (but not available for selection in the **Table type** drop-down list). These tables cannot be modified or deleted.

Normal low range

This field displays with the Basic Custom table type. Enter the normal low resistance range. The lowest value cannot be less than 51 ohms.

Normal high range

This field displays with the Basic Custom table type. Enter the normal high resistance range. The highest value cannot not exceed 12499 ohms. 10K (9999 ohms) is the recommended maximum resistance value for **Normal high range**. However, values up to 12.5K (12499 ohms) are allowed but will affect the accuracy of detection.

Normally open

This field displays with the Basic Custom table type.In add or modify mode, selecting this check box indicates that this circuit is normally open.

Priority code

This field displays with the Advanced Custom table type.In add or modify mode, select a priority code; low, medium or high.

Status code

This field displays with the Advanced Custom table type.In add or modify mode, select status codes. They are:

- **Inactive** - This is the normal state of the circuit.
- **Active** - This is the “alarm” state of the circuit.
- **Ground fault** - Supervisory Fault: “ground fault.” One (or both) lines is (are) grounded.
- **Shorted** - Supervisory Fault: “shorted circuit”
- **Open** - Supervisory Fault: “open circuit”
- **Foreign** - Supervisory Fault: “foreign voltage.” Represents any abnormal resistance not covered by the above definitions.
- **Non-settling** - Supervisory Fault “non-settling error.” Represents an oscillating condition (AC noise) where the circuit does not settle into any of the above states long enough to meet the “debounce” requirements.

Resistance range

This field displays with the Advanced Custom table type. In add or modify mode, for each range, two resistance values can be used. You can enter a numeric value or select a special resistance code from the drop-down list. The special resistance codes are:

- **Infinite** - infinite resistance
- **Shorted** - shorted line
- **Ground A** - ground line a
- **Ground B** - ground line b

The lowest value cannot be less than 50 ohms and the highest value cannot exceed 25,000 ohms.

Default

Resets the fields to the settings of a normally closed, 1K/2K circuit. This field is not enabled when you are viewing system type tables.

Add
Adds an EOL resistor table.

Modify
Modifies a custom EOL resistor table entry. System type tables cannot be modified.

Delete
Removes a custom EOL resistor table entry. System type tables cannot be deleted. Custom type tables cannot be deleted if they are in use by an input.

Help
Displays online help for this form.

Close
Closes the EOL Tables folder.

EOL Resistor Tables Form Procedures

Use the following procedures on this form.

Add an EOL Resistor Table

1. From the ***Access Control*** menu, select ***EOL Resistor Configuration***.
2. On the EOL Resistor Table form, click [Add].
3. If segmentation is not enabled on your system, skip this step. If segmentation is enabled on your system, the Segment Membership window opens. Select which segment you want this table to belong to and click [OK].
4. In the **Table name** field, type a name for the table. The name can contain a maximum of 32 characters.
5. From the **Table type** drop-down list, select the type of table that you want to add.
6. If you selected **Advanced Custom** from the **Table type** drop-down list, proceed to step 7.

   If you selected **Basic Custom** from the **Table type** drop-down list:
   a. Enter a normal low resistance range. The lowest value should not be less than 51 ohms.
   b. Enter a normal high resistance range. The highest value should not exceed 12499 ohms.
   c. If you want to indicate that the circuit is normally open, select the **Normally open** check box.

Note: Click [Default] if you want to reset the **Normal low range**, **Normal high range**, and **Normally open** fields to the settings of a normally closed, 1K/2K circuit.

7. If you selected **Advanced Custom** from the **Table type** drop-down list:
   a. Select the priority codes.
   b. Select the status codes.
   c. Select or enter the resistance ranges. The lowest value cannot be less than 50 ohms and the highest value cannot exceed 25,000 ohms.
8. Click [OK].

Modify an EOL Resistor Table

1. From the ***Access Control*** menu, select ***EOL Resistor Configuration***.
2. On the EOL Resistor Tables form, from the listing window, select the currently defined EOL resistor table that you want to modify.

Note: System type tables cannot be modified.

3. Click [Modify].
4. Make the changes you want to the fields. For more information, refer to EOL Resistor Tables Form on page 820.
5. Click [OK].

Delete an EOL Resistor Table

1. From the ***Access Control*** menu, select ***EOL Resistor Configuration***.
2. On the EOL Resistor Tables form, from the listing window, select the currently defined EOL resistor table that you want to remove.

Note: System type tables cannot be deleted. Custom type tables cannot be deleted if they are currently in use by an input.

3. Click [Delete].
4. Click [OK].

CHAPTER 40

Destination Assurance Folder

The Destination Assurance folder contains the Destination Assurance form with which you can:

- Associate entrance readers with exit readers.
- Configure a specific amount of time a cardholder is allowed to reach a specified exit reader before an alarm is generated.

This folder is displayed by selecting ***Destination Assurance*** from the ***Access Control*** menu.

Note: In order to enable the destination assurance feature, the Linkage Server must be configured and running.

Destination Assurance on Segmented Systems

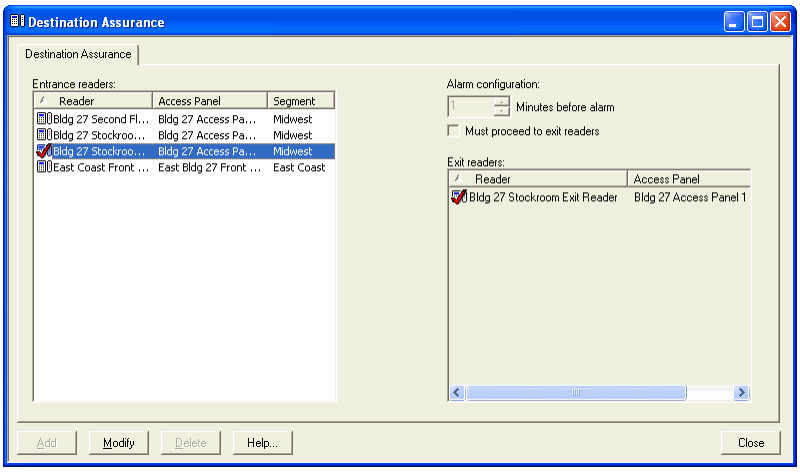
If a system is segmented, a user can only configure destination assurance for those entrance/exit readers that the user has access to. Also, to modify the “Minutes before alarm” and/or the “Must proceed to exit readers” settings on a segmented system, the user must have segment access for all configured exit readers that belong to the selected entrance reader.

For example, if an entrance reader has an exit reader from segment 1 and another exit reader from segment 2, a user who wishes to modify this value must have segment access to both segment 1 and 2. If the user does not have segment access to both segments and they try to change this setting, an error message that says the following will be displayed:

“You do not have segment access for one or more exit readers configured for this entrance reader. The ‘Minutes before alarm’ and ‘Must proceed to exit readers’ settings will not be saved.”

If a user does not have segment access for all configured exit readers, the user cannot modify the entrance reader settings. However, the user can still assign or remove exit readers for which they do have segment access to.

Destination Assurance Form



Entrance readers listing window

Lists currently defined readers and the name of the access panel connected to each. On segmented systems, the segment is displayed if you are logged in as an <All segments> user, but not if you are logged into a specific segment.

___ Minutes before alarm

After a cardholder enters an area at an entrance reader, they will have a certain amount of time to reach an associated exit reader before an alarm is generated. In modify mode, enter the time (in minutes) that you want to allow a cardholder to reach (one of) the selected entrance reader's associated exit reader(s). Enter a value between 1 and 9999. The default is 1. If the specified time elapses without the cardholder receiving a grant at a valid exit reader, the reported alarm will be: "User Failed to Reach Destination."

Segmented systems only: To modify this value (and the **Must proceed to exit readers** check box) on a segmented system, the user must have segment access for all configured exit readers that belong to the selected entrance reader.

For example, if an entrance reader has an exit reader from segment 1 and another exit reader from segment 2, a user who wishes to modify this value must have segment access to both segment 1 and 2. If the user does not have segment access to both segments and they try to change this setting, an error message that says the following will be displayed: "You do not have segment access for one or more exit readers configured for this entrance reader. The 'Minutes before alarm' and 'Must proceed to exit readers' settings will not be saved."

Must proceed to exit readers

Select this check box to indicate that a cardholder must go to one of the specified exit readers. If this check box is selected and a cardholder attempts to gain access or gains access to any other reader besides an exit reader associated with the selected entrance reader, an alarm will be generated.

If a cardholder is granted access at an unexpected reader, the reported alarm will be: "Unexpected Access." If a cardholder attempts to gains access at an unexpected reader, the reported alarm will be: "Unexpected Access Attempt."

It is important to note that since the destination assurance feature is configurable on multiple controllers, it is possible that false alarms could be reported if the entrance and exit readers are on separate controllers and one, but not both, of these controllers is offline.

If the **Destination exempt** check box was selected for a badge on the Badge form in the Cardholders folder, the badge will not be included in the destination assurance processing and no alarms will be generated if the cardholder violates any of the destination assurance settings.

Segmented systems only:

To modify this value (and the Minutes before alarm setting) on a segmented system, the user must have segment access for all configured exit readers that belong to the selected entrance reader.

For example, if an entrance reader has an exit reader from segment 1 and another exit reader from segment 2, a user who wishes to modify this value must have segment access to both segment 1 and 2. If the user does not have segment access to both segments and they try to change this setting, an error message that says the following will be displayed: “You do not have segment access for one or more exit readers configured for this entrance reader. The ‘Minutes before alarm’ and ‘Must proceed to exit readers’ settings will not be saved.”

Exit readers listing window

In view mode, lists all exit readers that have been associated with the selected entrance reader and the name of the access panel connected to each. On segmented systems, the segment is is displayed if you are logged in as an <All segments> user, but not if you are logged into a specific segment.

In modify mode, lists all readers and the name of the access panel connected to each. On segmented systems, the segment is is displayed if you are logged in as an <All segments> user, but not if you are logged into a specific segment.

Add

This button is not used.

Modify

Click this button to

Delete

This button is not used.

Help

Click this button to display online help for this form.

Close

Click this button to close the Destination Assurance folder.

Destination Assurance Form Procedures

Use the following procedures on this form.

Configure Destination Assurance

1. From the ***Access Control*** menu, select ***Destination Assurance***. The Destination Assurance folder opens.
2. From the Entrance readers listing window, select a reader.
3. Click [Modify].
4. From the Exit readers listing window, select one or more readers.

Note: The entrance reader and exit readers do not have to exist on the same controller.

5. After a cardholder enters an area at an entrance reader, they will have a certain amount of time to reach an associated exit reader before an alarm is generated. In the **___ Minutes before alarm** field, for the selected entrance reader, enter the time (in minutes) that you want to allow a cardholder to reach (one of) the associated exit readers you selected in step 4. Enter a value between 1 and 9999. The default is 1.

Notes: To modify this value on a segmented system, the user must have segment access for all configured exit readers that belong to the selected entrance reader.

If the specified time elapses without the cardholder receiving a grant at a valid exit reader, the reported alarm will be: "User Failed to Reach Destination"

6. Select the **Must proceed to exit readers** check box to indicate that a cardholder must go to one of the specified exit readers. If this check box is selected and a cardholder attempts to gain access or gains access to any other reader besides an exit reader associated with the selected entrance reader, an alarm will be generated.
   - If a cardholder is granted access at an unexpected reader, the reported alarm will be: "Unexpected Access"
   - If a cardholder attempts to gains access at an unexpected reader, the reported alarm will be: "Unexpected Access Attempt"

Notes: To modify this value on a segmented system, the user must have segment access for all configured exit readers that belong to the selected entrance reader.

It is important to note that since the destination assurance feature is configurable on multiple controllers, it is possible that false alarms could be reported if the entrance and exit readers are on separate controllers and one, but not both, of these controllers is offline.

If the **Destination exempt** check box was selected for a badge on the Badge form in the Cardholders folder, the badge will not be included in the destination assurance processing and no alarms will be generated if the cardholder violates any of the destination assurance settings.

7. Click [OK].

Note: Via the Reports folder, you can run a Destination Assurance Exempt Cardholders report to see a list of which cardholders will be exempt from processing, or a Destination Assurance Configuration report to display a list of all configured entrance readers and their settings as well as the associated exit reader(s) for each entrance reader.

CHAPTER 41

Selective Cardholder Download

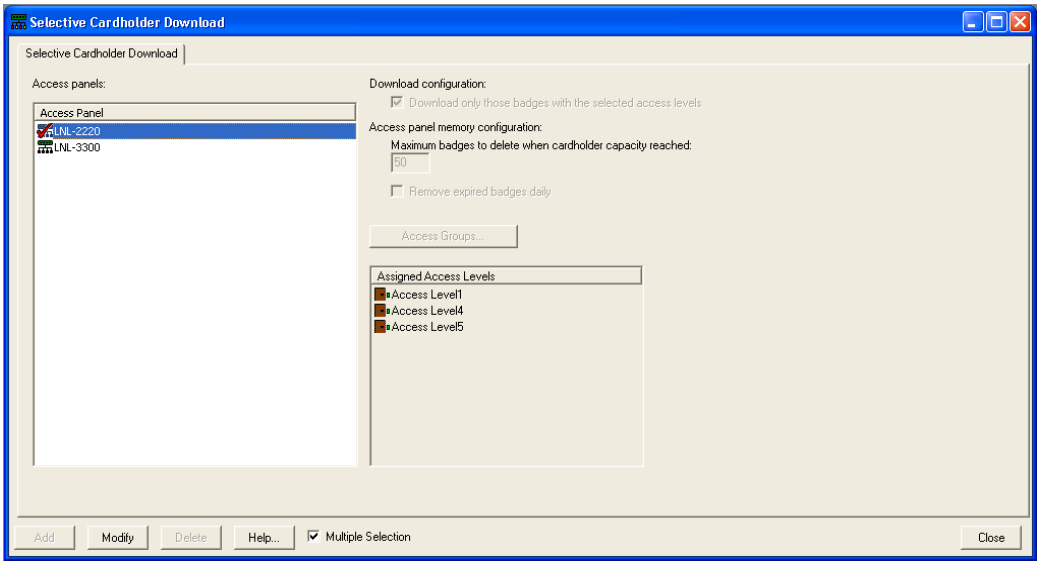
The Selective Cardholder Download folder is used to specify which access levels a badge must have assigned to it in order to be downloaded to the selected access panel. This feature makes it much easier to add cardholders to a panel for specific access levels without having to download the entire database.

Use this feature for installations with a large cardholder database when you only need a subset of those cardholders downloaded to an access panel.

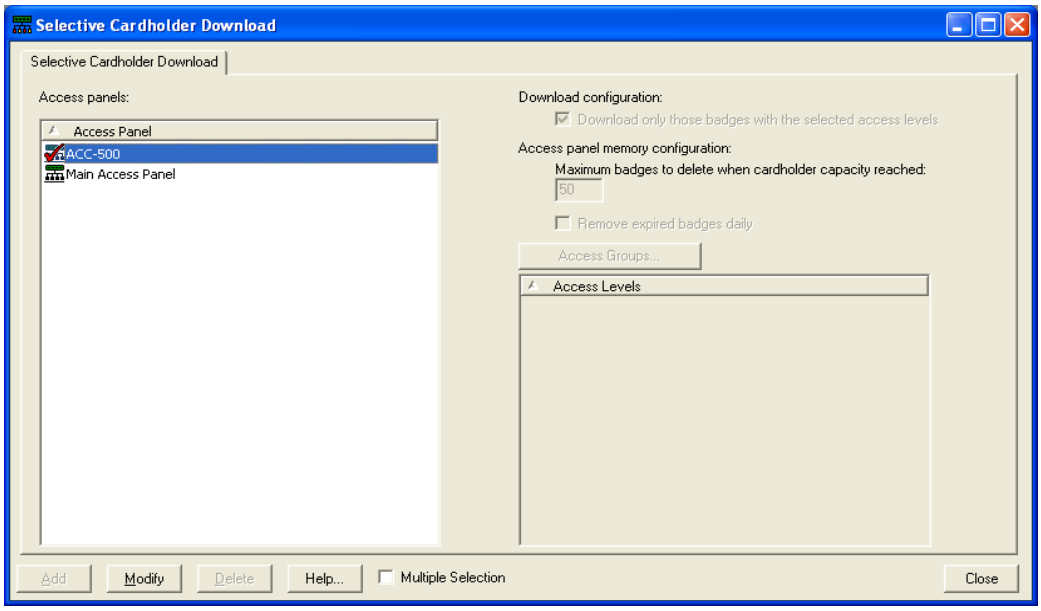
Note: When an access panel has selective cardholder download enabled, the icon in Alarm Monitoring will display as:

Selective Cardholder Download Form

Selective Cardholder Download Form (View Mode)



Selective Cardholder Download Form (Modify Mode)



Access Panel

Lists the access panels currently installed on the system.

Download only those badges with the selected access levels

Select this to configure the download to only download those badges with access levels that you placed in the Assigned Access Levels list below.

Maximum badges to delete when cardholder capacity reached

Enter the number of badges to delete when the panel's cardholder capacity is reached. For example, if this field is set to 30, and the capacity for badges is reached in the panel, then 30 badges that had been added "on-demand" will be deleted starting with those with the oldest expiration date. The minimum value for this field is 1. For more information, refer to Cardholders Added to Panels "On-Demand" on page 832.

Remove expired badges daily

Select this check box to remove expired badges that were added "on-demand" from the panel.

Access Groups

Opens the Select Access Levels in a Group window. Use this window to select the access group whose levels you want to select or unselect. Access levels belonging to the access group will be automatically selected in both the Available and Assigned Access Levels lists.

Available Access Levels

Lists the access levels available for the selected panel. By default, this list will only show access levels that include readers attached to the panel. Alternatively, you can use the **Show all access levels** option. For more information, refer to Show all access levels on page 831.

Assigned Access Levels

Lists the access levels you have assigned for the selective cardholder download.

Show all access levels

Select this check box to view and select from all access levels currently configured in the segment to which the panel belongs. When more than one panel is selected, **Show all access levels** is always enabled.

Multiple Selection

If selected, more than one panel in the same segment can be selected simultaneously. The changes made on this form will apply to all selected panels.

Assign

Moves selected entries from the Available Access Levels list to the Assigned Access Levels list.

Remove

Removes selected entries from the Assigned Access Levels list.

Modify

This button is used to change an existing selective cardholder download assignment.

Close

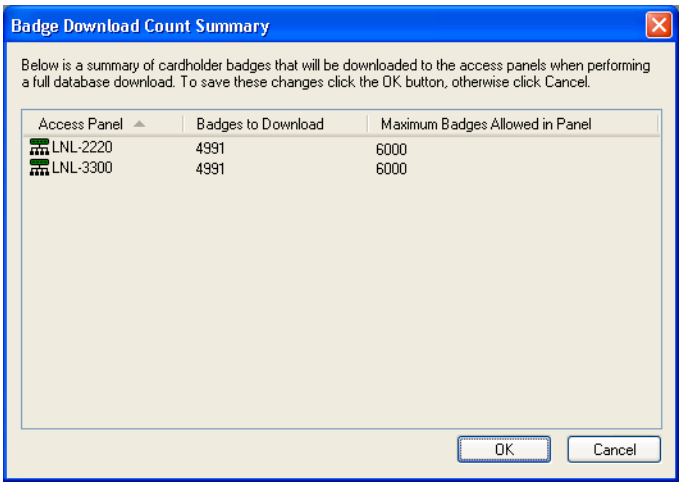
Closes the Selective Cardholder Download folder.

Help

Displays online assistance for this form.

Configuring a Selective Cardholder Download

1. Select an access panel from the Access Panel listing window. The access levels assigned for selective download to that panel will be listed.
2. Click [Modify]. By default, only access levels related to the selected panel will be listed in the Available Access Levels listing window. (Panel-related access levels are those assigned to devices that are defined on the panel.)
3. Optionally, select the **Show all access levels** check box to display all access levels in configured in OnGuard.
4. Select the **Download only those badges with the selected access levels** check box.
5. Optionally, you can enter the **Maximum badges to delete when cardholder capacity reached**. Use a small enough maximum number so the system does need to spend time deleting a large number of badges if only a few need to be deleted.
6. Optionally, you can choose to remove expired badges from the system (they will be purged from the system nightly) by selecting the **Remove expired badges daily** check box.
7. From the Available Access Levels list, select one or more access levels that you want to assign to the panel.
8. Click [Assign] to move the selected access levels to the Assigned Access Levels list.
9. Click [OK] to save the changes and return to the view mode.
10. If you configured selective download for multiple panels, the Badge Download Count Summary dialog is displayed. Verify that the Badges to Download is not greater than the Maximum Badges Allowed in Panel, then click [OK] to save the changes.



Cardholders Added to Panels “On-Demand”

Once configured, only cardholders that have an access level assigned in the selective download will be downloaded to the panel during a full database download. You must initiate a database download to the panel manually before any badge filtering is applied.

Cardholders that have an access level that contains one or more readers defined on the panel, but do not exist in the panel due to the selective download configuration, will be added to the panel “on-demand” as they attempt to gain access to the readers that exist for the panel.

A cardholder that is added to the panel “on-demand” may have to use their badge 2 or 3 times before they are downloaded to the panel and granted access.

If a panel that supports selective cardholder downloads reaches its maximum cardholder capacity, the following will occur:

- The Communication Server will delete all badges from the panel that do not have a selective level assigned.
- The Max Cardholders Reached event will be reported in Alarm Monitoring.
- If you have configured this option, a specified number of expired badges will be deleted from the system.

Notes:

When a badge that will be downloaded “on-demand” is presented to one of the readers defined on the panel, the event “Denied, Badge Not In Panel” will be reported in Alarm Monitoring. This event will be reported for each access attempt by the badge until the badge has been successfully downloaded.

The Selective Cardholder Download “on-demand” badge downloading is only supported for direct and LAN connections to the access panel and NOT dialup. The Selective Cardholder Download database download feature is supported for all connection types, including dialup, assuming a dialup connection has been established with an access panel.

A badge MUST be used for the “on-demand” badge download to work. If a cardholder attempts to gain access to a selective download panel using only a PIN code, the on-demand badge download will not work.

You can configure a Selective Cardholder Download without choosing an access level. If you do this, no badges will be downloaded to a panel during a full database download.

They will be downloaded only “on-demand” as long as the badge has access to a reader for the panel.

When a badge is added or modified with selective cardholder download enabled, and if the badge has an access level assigned to the panel’s selective download list, the badge will be added to the panel. Otherwise the badge will be deleted from the panel.

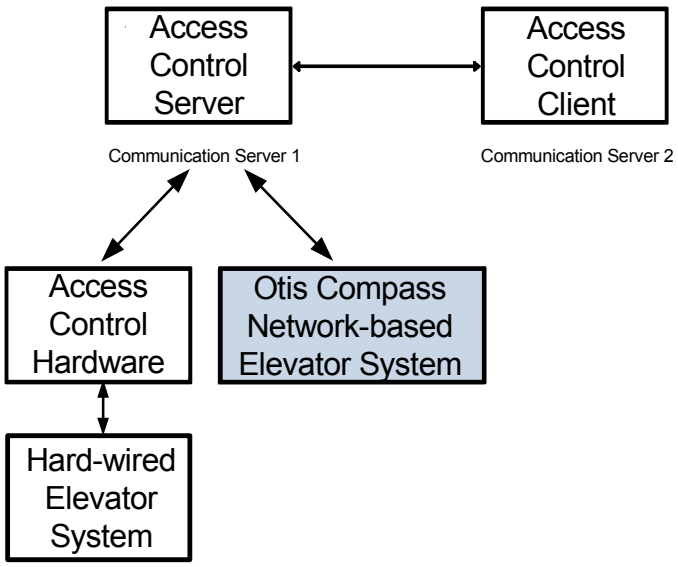
Any badge that is only assigned a temporary access level should be removed from the panel after the access level expires.

CHAPTER 42

Elevator Dispatching Configuration Folder

This section describes the configuration of an Otis Compass network-based elevator system.

For hard-wired elevator systems: Use the Elevator Hardware form to configure various Lenel hardware solutions including the LNL-1300 panel (6 floors; no floor tracking) or LNL-1320 panel (128 floors; floor tracking optional). For more information, refer to Elevator Hardware Form Procedures on page 674.

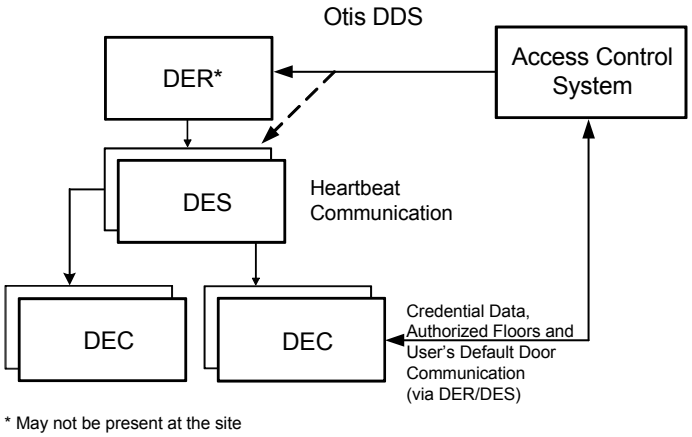


The Elevator Dispatching Configuration form is used to integrate OnGuard with the Otis Elevator's Destination Dispatch System (DDS).

DDS includes the following components:

- **Destination Entry Computer (DEC)** - a touch screen or keypad that acts as a communication channel between the user and an elevator in the system. In OnGuard, DEC is referred to as Elevator Terminal and is configured as a device associated with an Elevator Dispatching Device (DES or DER).

- **Destination Entry Redirector (DER)** - supports elevators (DECs) that are not part of an elevator group. The DER connects to all elevator groups and allows DECs at a common entry point in the building, such as a lobby, to accept destination requests for any floor in the building.
- **Destination Entry Server (DES)** - controls a group of elevators. Each elevator group has a primary DES and, optionally, a standby or backup DES for the situation when the primary DES is down.



This solution addresses the secure access requirements of high-rise buildings as well as efficient movement of traffic to various elevator banks.

Elevator Dispatching Configuration Overview

OnGuard integrates with DDS by passing information onto the DDS and allowing it to implement its own logic to perform functions, which include determining if an elevator cab is called based on an access attempt or if a person is allowed to proceed to a floor without presenting any security credentials.

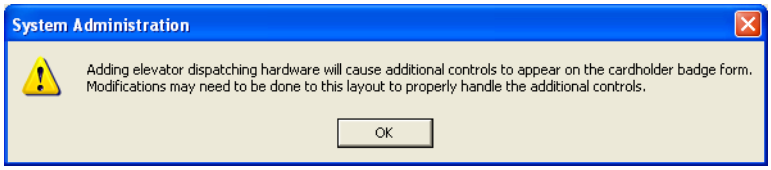
Note: It must be noted that the DDS is composed of many third-party hardware devices. OnGuard is not responsible for the operation, setup, or configuration of these third-party hardware devices. OnGuard is just transmitting messages to the DDS.

Elevator Dispatching User Permissions

Permissions for elevator dispatching can be given or restricted through System Administration. From the ***Administration*** menu select ***Users***. On the System Permission Groups tab, you can grant or deny elevator dispatching. For more information, refer to System Permission Groups Form on page 361.

Elevator Dispatching and the Cardholder Badge

The first time you configure elevator dispatching hardware, additional controls are automatically added to the Cardholder Badge form and the following message is displayed:

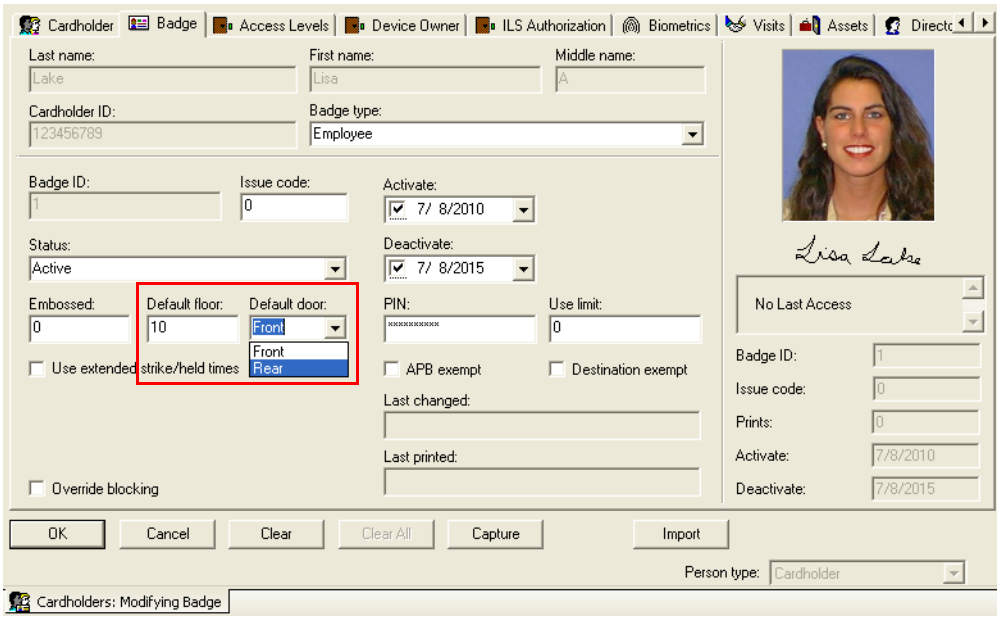


Check the Cardholder Badge form to ensure the additional controls do not interfere with the existing fields. If necessary, use FormsDesigner to adjust the Badge form layout.

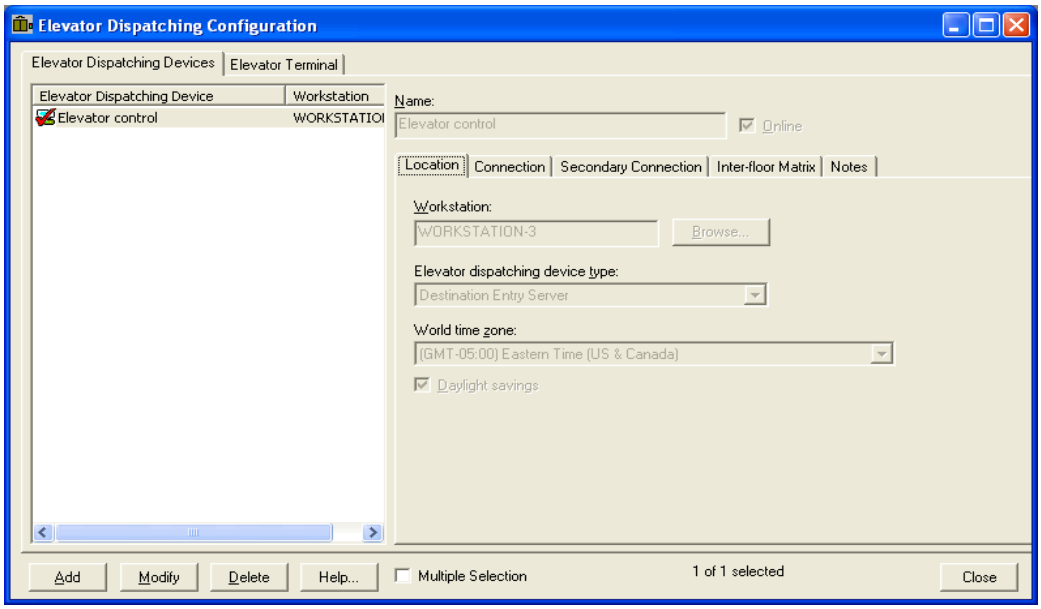
Enterprise systems: In Enterprise environments, it is required that all forms changes be done at the Master. Therefore, when adding Elevator Dispatching hardware to a Region, the additional controls are not added automatically. As part of setting up the system, you must use FormsDesigner to add the following **System Objects (Default floor and Default door)** to the Master database, and then replicate the forms down to all Regions. For details on how to add system objects to forms, refer to the Form Editing Procedures chapter in the FormsDesigner User Guide.

Cardholder Badge Form Configuration Instructions

In the System Administration menu bar, select ***Administration*** > ***Cardholders***. On the Badge sub-tab, the **Default floor** field and **Default door** drop-down allow you to configure the cardholder's default floor and elevator door. For more information, refer to Badge Form on page 109.



Elevator Dispatching Devices Form (Location Sub-tab)



Listing window

Lists currently defined elevator dispatching devices and the name of the workstation that is connected to each.

Name

Identifies the name of the elevator dispatching device. This is a “friendly” name assigned to each elevator dispatching device to make it easy to identify. Each name must be unique.

Online

If selected, the elevator dispatching device will be online. Online indicates that the elevator dispatching device is ready for use, and that the Communication Server will attempt to communicate with the device. If the elevator dispatching device is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Select the workstation or server to which the elevator dispatching device is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation.

You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Elevator dispatching device type

Choose either:

- Destination Entry Server. This is a server that controls a group of elevators and is responsible for communicating with Destination Entry Computer (DEC) keypad terminals.
- Destination Entry Redirector. This is a server that is associated with all elevator groups in an entire building. This can communicate with global Destination Entry Computer (DEC) elevator terminals.

World time zone

Select the world time zone for the selected elevator dispatching device's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

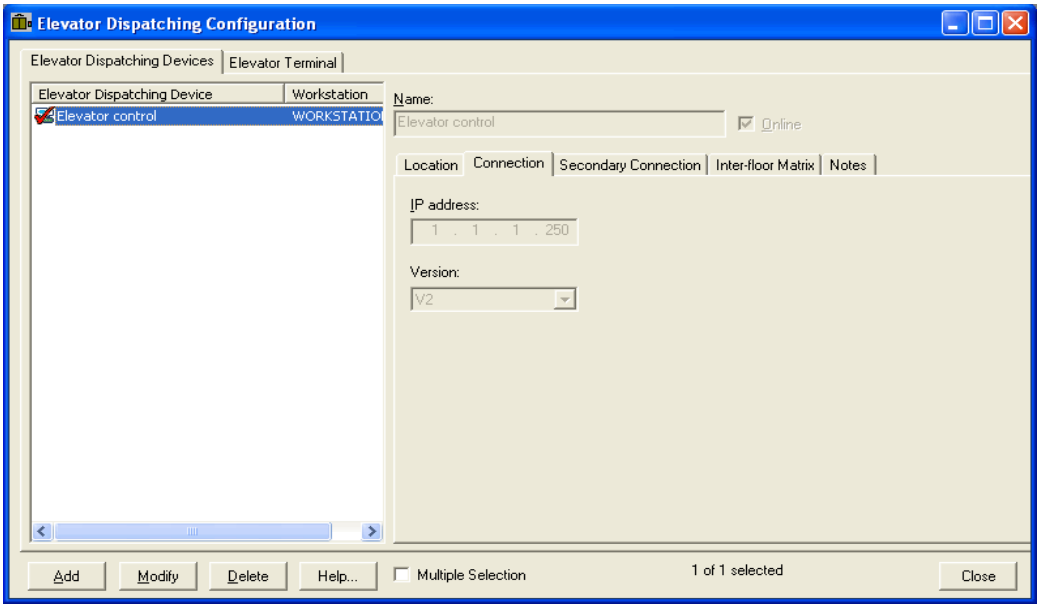
- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

The world time zone is only used for reporting purposes on the elevator dispatching server side.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected elevator dispatching device's geographical location.

Elevator Dispatching Devices Form (Connection Sub-tab)



IP address

Enter the Internet Protocol (TCP/IP) address for the elevator dispatching device, as provided by your LAN Network Administrator.

An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number.

The elevator dispatching device itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the elevator dispatching device.

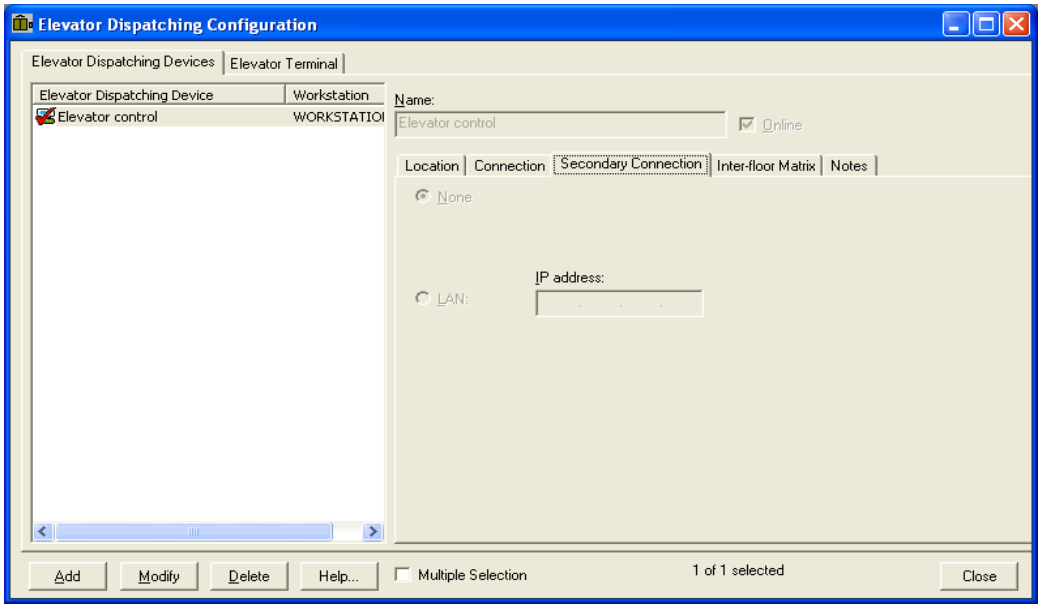
Version

Select which version of the DES or DER firmware and their associated DEC devices are installed in your system. Both "V1" and "V2" systems are supported.

If version V1 does not fully support a feature in OnGuard, only the applicable information will be sent to the V1 devices (V2-specific settings will be ignored.)

Elevator Dispatching Devices Form (Secondary Connection Sub-tab)

Note: The secondary connection is used when the primary connection fails.



None

Select if you do not want a secondary connection.

LAN

Select this radio button so the workstation can communicate with the elevator dispatching device over a Local Area Network. You must also specify the workstation's IP address.

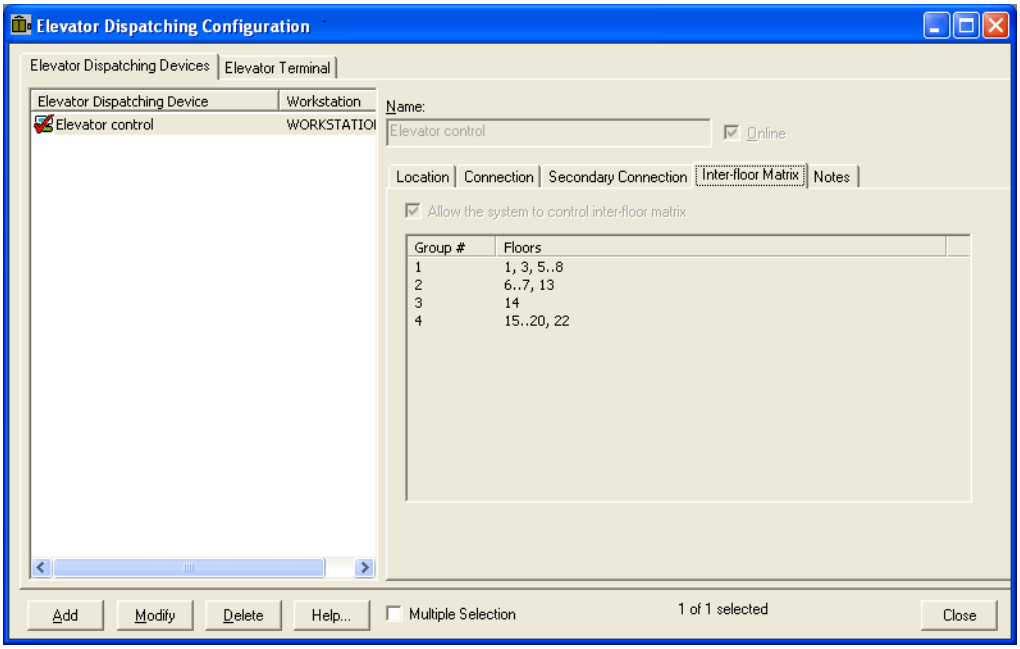
IP address

The secondary IP address only applies to a DES that is configured as a failover DES. This is the DES that takes over in the event that the primary DES goes offline.

Enter the Internet Protocol (TCP/IP) address for the elevator dispatching device, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number.

The elevator dispatching device itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the elevator dispatching device.

Elevator Dispatching Devices Form (Inter-floor Matrix Sub-tab)



Allow the system to control inter-floor matrix

Select this check box to use OnGuard to configure the floors of a building into logically divided sections (floor groups) to prevent passenger requests between the designated sections of the building, and possibly, to separate passengers into different elevator cars based on their section membership. Examples:

- A 10-story apartment building is configured into two apartment complexes (sections). The first complex consists of apartments located on floors 2 through 5. The second complex consists of apartments on floors 6 through 10. In this scenario, if a passenger request is made at floor 2, the elevator will only serve floors 3, 4, or 5. If a passenger request is made at floor 6, the elevator will only serve floors 7, 8, 9, or 10.
- VIP clients of a building or business are granted exclusive access to an elevator car.

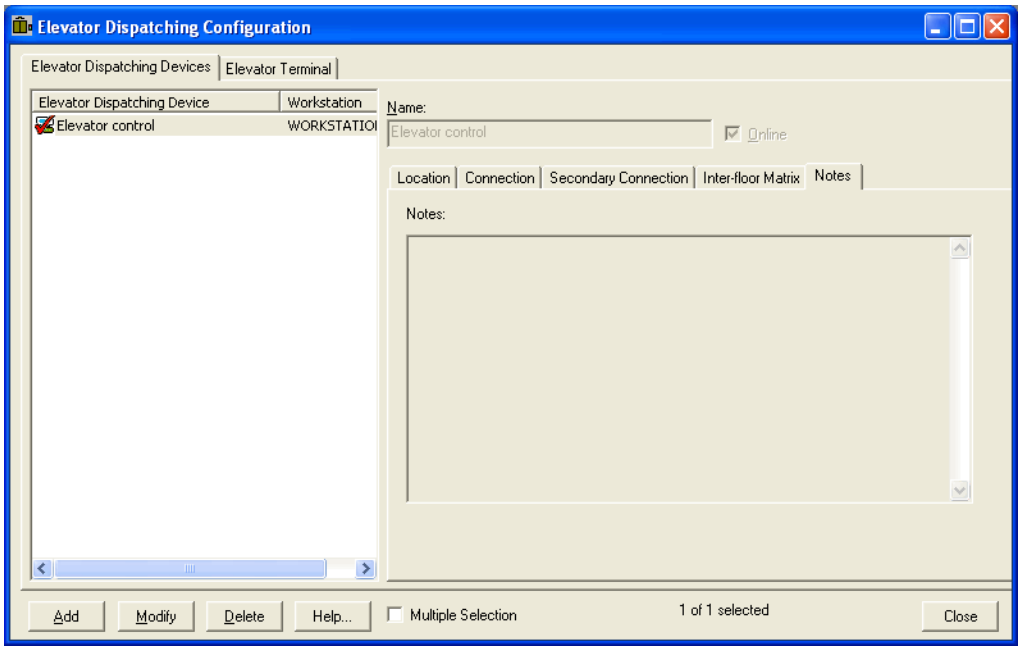
This check box is only available for version “V2” DES devices.

Listing window (inter-floor matrix)

In the add or modify mode, allows you to specify up to four (4) floor groups per DES. In the view mode, lists the currently defined floor groups.

- **Group #** - Identifies the group of floors (section) of the building. The group number is automatically generated when you add a new group.
- **Floors** - Specifies the floor numbers in the group.

Elevator Dispatching Devices Form (Notes Sub-tab)



Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide.

Elevator Dispatching Devices Form Procedures

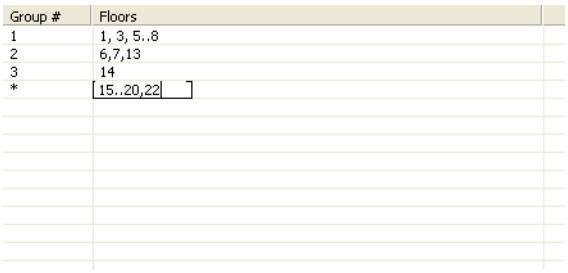
Use the following procedures on this form.

Add an Elevator Dispatching Device

1. Display the Elevator Dispatching Configuration folder by selecting ***Elevator Dispatching*** from the ***Access Control*** menu. Make sure the Elevator Dispatching Devices tab is selected.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the elevator dispatching device.
4. If you want to place the elevator dispatching device online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system, but instead would wait until you're ready to put the panel into service.
5. Specify communication parameters on the Location, Connection, and Secondary Connection sub-tabs.
6. For version V2 DES devices only: If you are configuring passenger separation, complete the following steps on the Inter-floor Matrix sub-tab:
   a. Select the **Allow the system to control inter-floor-matrix** check box.
   b. Double-click in the add row (*) to add a group of floors.

c. Type the floor numbers you want to include in the group. The floor numbers must be comma-separated and sequential floor numbers can be entered as a range of numbers. For example, if Group # 4 includes floor numbers 15, 16, 17, 18, 19, 20, and 22, you can type this information as follows:

```
15..20,22
```



Note: Whichever format you use to type the floor numbers (individually or as a range of numbers), the system will merge consecutive floor numbers into the range format. For example, if you type `2..10,11,15` and then click [OK] to save the form, the results will display as `2..11,15`.

d. Press <Enter>. The **Group #** will be generated automatically.

e. Continue using the add row (*) to add more floor groups until you have configured all of the elevator's floor groups.

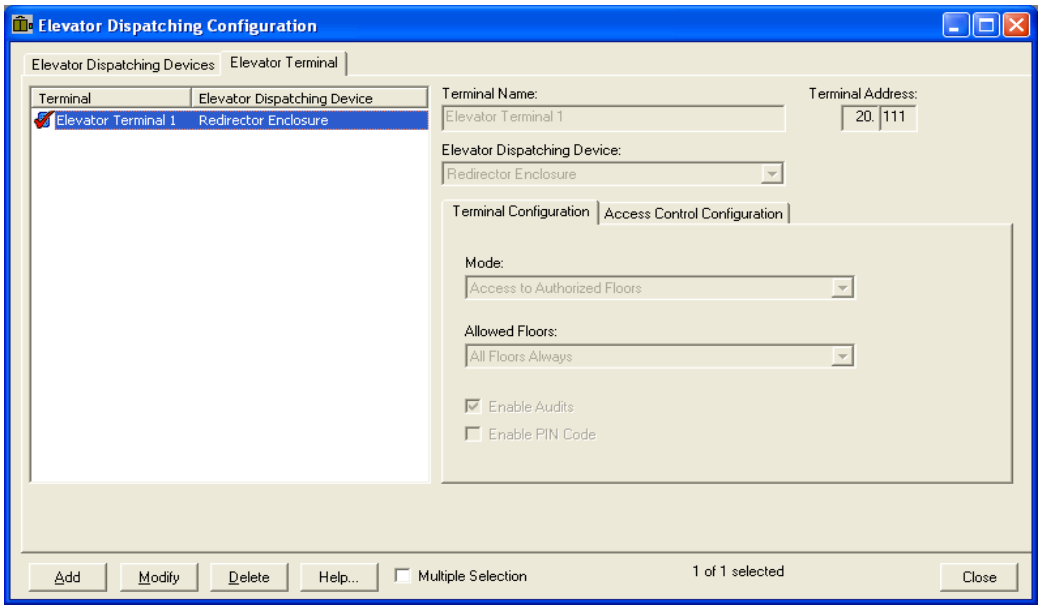
Note: Each DES elevator dispatching device can have up to four (4) floor groups configured for it.

7. Click [OK].

Enter Notes

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Elevator Terminal Form (Terminal Configuration Sub-tab)



Listing window

Lists currently defined elevator terminal devices and the name of the elevator dispatching device to which each is associated.

Terminal Name

Identifies the name of the terminal. This is a “friendly” name assigned to each terminal to make it easy to identify.

Terminal Address

Enter the last two sets of numbers from the IP address of the terminal.

Elevator Dispatching Device

Choose the Elevator Dispatching Device that is used with the terminal.

Mode

Refers to operational modes which dictate how the elevator terminal interacts with the cardholder. Choose from:

- **Access to Authorized Floors**: When the cardholder presents a valid badge to the elevator reader, and then selects an authorized floor, the system calls the authorized floor.
- **Default Floor Only**: When the cardholder presents a valid badge to the elevator reader, or enters a valid PIN code or floor number on the DEC (elevator terminal), the system calls the default floor.
- **Default Floor or User Entry of Destination Floor**: When the cardholder presents a valid badge to the elevator reader, the system calls the cardholder's default floor. Within a configurable timeout period, the cardholder can override the default floor call by entering another floor number.
- **User Entry of Destination Floor**: The cardholder has the option to select a floor with or without presenting their badge to the elevator reader. If the selected floor is an allowed floor, the system calls the floor. If the floor is a non-allowed floor, the cardholder is requested to present their badge.

Allowed Floors

Allowed floors are floors that can be accessed via the elevator terminal without supplying security credentials. An example may be a common floor such as a lobby or parking garage. Select from the user-defined or system (“All Floors Always” and “No Floors”) entries.

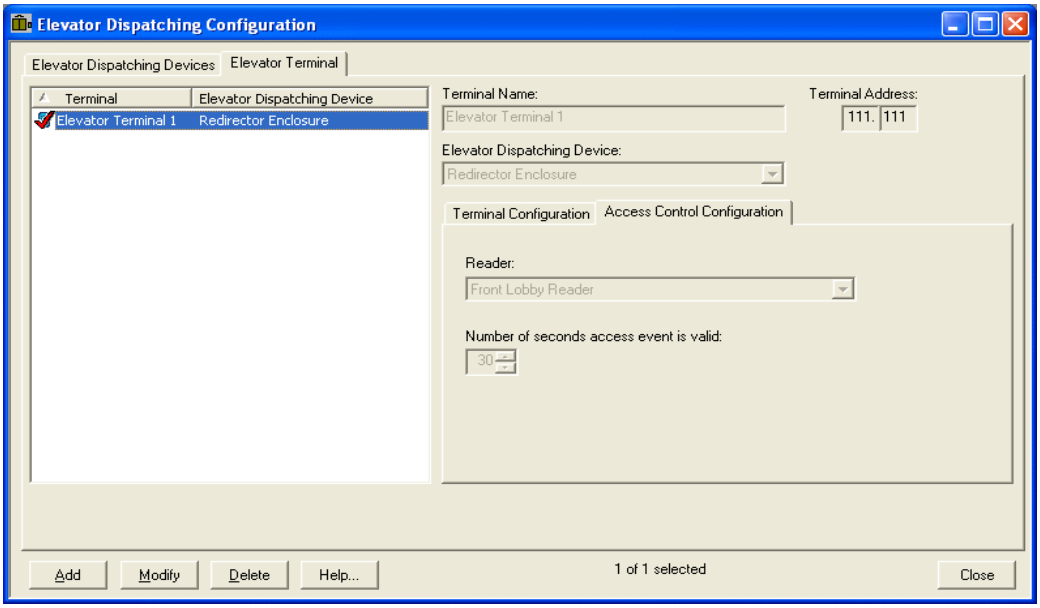
Enable Audits

Select to allow events to be sent from the DEC (elevator terminal) to Alarm Monitoring. This feature is only available for elevator terminals associated with version “V2” DES or DER devices.

Enable PIN Code

Select to allow the cardholder to enter their personal identification number (PIN) from the DEC (elevator terminal). If a valid PIN code is entered, OnGuard will send the authorized floors to the DEC based on the badge's access levels. This feature is only available for elevator terminals associated with version “V2” DES or DER devices.

Elevator Terminal Form (Access Control Configuration Sub-tab)



Reader

Select the reader that is to be associated with the elevator terminal. Any access activity, from the reader, that is specific to the Destination Dispatching System will be sent to the elevator terminal. For the configured elevator to receive a call from OnGuard, an access granted with access event type must be received for the reader assigned to the elevator.

Number of seconds access event is valid

Sets the time frame (in seconds) for which an access attempt is considered valid if the reader/host goes offline.

Elevator Terminal Form Procedures

Use the following procedures on this form.

Add a Terminal

1. Display the Elevator Dispatching Configuration folder by selecting ***Elevator Dispatching*** from the ***Access Control*** menu. Make sure the Elevator Terminal tab is selected.
2. Click [Add].
3. In the **Terminal Name** field, type a unique, descriptive name for the elevator terminal.
4. Specify the terminal address.
5. Specify what elevator dispatching device the terminal will be associated with by using the **Elevator Dispatching Device** drop down box.
6. Specify the options on the Terminal Configuration and Access Control Configuration sub-tabs.
7. Click [OK].

Monitoring

CHAPTER 43

Alarm Configuration Folder

The Alarm Configuration folder contains forms with which you can:

- Define a set of alarms that can be sent to an alarm monitoring workstation.
- Define alarm links for each alarm (the set of events that cause that alarm to be sent.) The set of events for an alarm can be optionally restricted to:
  - Events with certain parameter values (parameter-based events).
  - Events generated by specific hardware (within that segment if the database is segmented).
- Define custom alarms (not defined in the OnGuard database by default).
- Define how alarm monitoring stations display alarms.
- Assign a priority to an alarm.
- Select options that control the behavior of an alarm in Alarm Monitoring
- Group linked hardware devices with custom alarms.
- Password-protect alarm display and acknowledgment.
- For a particular alarm, specify text, sound, and camera instructions for monitoring purposes.
- Assign e-mail and page messages to an alarm.
- Link actions to alarms such that when an alarm is acknowledged the corresponding actions will be performed.

The folder contains eight forms: the Alarm Definitions form, the Alarm Configuration form, the Priority form, the Text form, the Audio form, the CCTV Instructions form, the Messages form and the Acknowledgment Actions form.

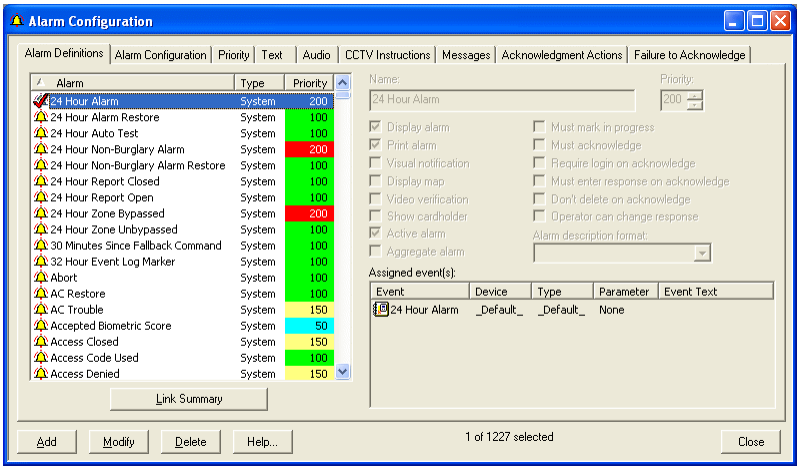
Toolbar Shortcut

The Alarm Configuration folder is displayed by selecting ***Alarms*** from the ***Monitoring*** menu or by selecting the Alarms toolbar button.

Alarm Definitions Form (View Mode)

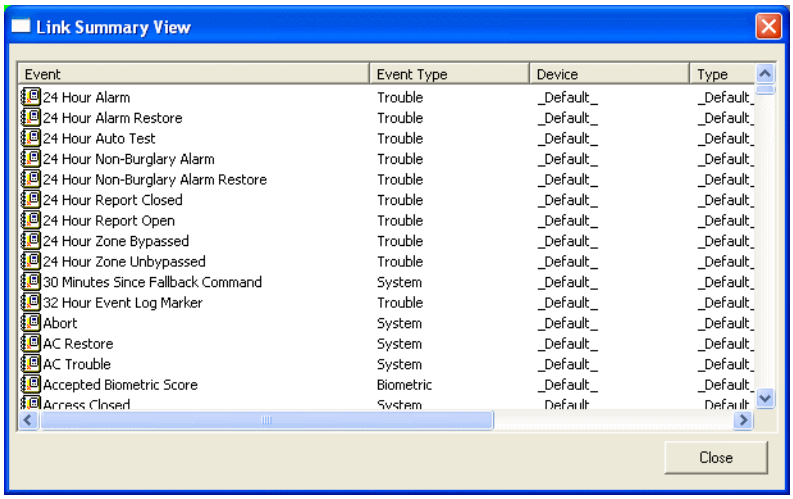
This form is used to:

- Assign a priority to an alarm.
- Select options that control the behavior of the alarm in Alarm Monitoring.
- Link specific hardware devices with events, and group them into custom alarms.

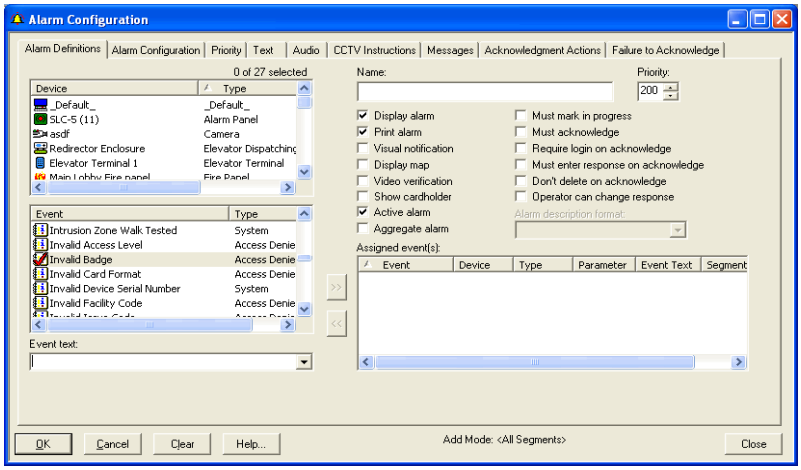


Link Summary View Window

This window is opened by clicking the [Link Summary] button on the Alarm Definitions form.



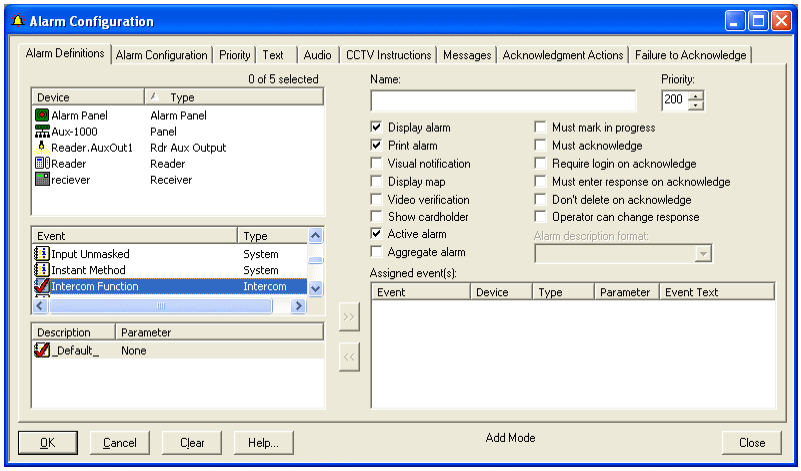
Alarm Definitions Form (Modify Mode for Normal Events)



Alarm Definitions Form (Modify Mode for Parameter-Based Events)

To open the Alarm Definitions form in modify mode for parameter-based events:

1. Click [Add] when the Alarm Definitions form is in view mode, and the display will change to Add (edit) mode for normal events.
2. In the Events display field, select a parameter-based event. (**Intercom Function**, **Transmitter Alarm**, **Transmitter Alarm Restored**, **Transmitter Low Battery**, **Transmitter Low Battery Restored**, **Transmitter Pre-Tilt**, **Transmitter Pre-Tilt Restored**, **Transmitter Pull Cord Alarm**, **Transmitter Pull Cord Restored**, **Transmitter Tamper**, **Transmitter Restored**, **Transmitter Tilt Disable**, **Transmitter Tilt**, **Transmitter Tilt Disabled**, **Transmitter Tilt Enabled**, **Transmitter Tilt Restored**, **Trouble Acknowledge**, **Trouble In**, and **Trouble Out** are the only parameter-based events.)
3. The **Access Control Events** display field will get smaller, and the **Event Parameters** display field will appear. The form will look like the following:



Display alarm

If selected, the alarm will be displayed on an alarm monitoring workstation when the corresponding event is triggered. If this box is not selected, such alarms will not be displayed in the listing.

Print alarm

If selected, a one-line entry will automatically be printed to an activity printer at an alarm monitoring workstation when the corresponding event is triggered. An activity printer must be configured for the monitoring workstation via the Workstations form in the System Configuration folder.

Visual notification

When the alarm arrives, the Main Alarm Monitor window will be displayed in the foreground on the Alarm Monitoring workstations. This feature can be disabled in Alarm Monitoring.

Display map

If selected, the monitoring map that contains the alarm's location is associated with that alarm. If the automatic map display option in Alarm Monitoring is also checked, a map will automatically display when that alarm occurs. This automatic map display feature can be disabled in Alarm Monitoring.

If this check box is selected in System Administration and in Alarm Monitoring, the map displays.

If this check box is selected in System Administration and not selected in Alarm Monitoring, no map displays.

If this check box is not selected in System Administration and not selected in Alarm Monitoring, no map displays.

If this check box is not selected in System Administration and selected in Alarm Monitoring, no map displays.

Video verification

Select if you want to show the video verify view for a given alarm upon arrival. The video verify view is only displayed if the alarm is so configured and if the instance of the alarm deals with a reader. A video board must be configured for the monitoring workstation via the Workstations form in the System Configuration folder.

Show cardholder

Select if you want to show the cardholder view for a given alarm upon arrival. If the cardholder screen is already being displayed when such an alarm comes in, it is brought to the foreground and the new cardholder associated with the alarm is searched. The cardholder screen is shown only if the alarm is so configured AND the instance of the alarm deals with a badge ID.

Active alarm

Selecting this check box produces the following effects in Alarm Monitoring: This alarm, when it occurs, will be highlighted in the Main Alarm Monitor window. The color of the highlight is determined by the priority value associated with the particular alarm. Priority values are specified on this form, but the color displayed for a given value is assigned on the Priority form of this folder. When this alarm occurs, animation displayed on the monitoring map for the associated device will indicate the location of the alarm. Next to the device icon, the word "Alarm" will grow to a maximum size, then the animation will pause before restarting.g

Aggregate alarm

Select this check box to combine all alarms of this type into one alarm in Alarm Monitoring. The alarm window columns will display the most recent alarm info. Actions will still be applied for individual alarms. Aggregation is only applied to the Main Alarm window, users can still perform a trace to see all alarms.

Note: After selecting this check box for an alarm, the alarm configuration must be refreshed in Alarm Monitoring before aggregation of alarms will begin.

Must mark in progress

Selecting this check box requires the alarm to be marked “in progress” in Alarm Monitoring. When the **Must mark in progress** check box is checked the **Must acknowledge** check box is automatically checked too.

Must acknowledge

When the alarm arrives, the alarm must be acknowledged before it can be deleted. If it’s an initiating alarm, the canceling alarm won’t be displayed until the initiating alarm is acknowledged.

Require login on acknowledge

If selected, the operator will be required to log in when (s)he attempts to acknowledge this alarm. The operator can log in using the same or a different user ID from that which was used at initial login. This login is used only for logging transactions related to the acknowledgment of the alarm.

Must enter response on acknowledge

If selected, the operator must enter an alarm response in the **Notes** field of the Alarm Acknowledgment window before the alarm can be acknowledged.

Don't delete on acknowledge

By default, an alarm is automatically deleted from the Main Alarm Monitor window upon acknowledgment. If this check box is selected, an acknowledged entry will be marked with a checkmark, but won't be deleted automatically. The operator must manually remove it by selecting ***Delete*** from the ***Edit*** menu.

It is important to note, however, that a canceling alarm will always automatically delete its corresponding initiating alarm (unless the operator deletes it first). The exception to this is an alarm for which the “Must acknowledge” check box is selected. A canceling alarm won’t delete such a Must acknowledge initiating alarm if it is unacknowledged.

Operator can change response

If selected, the operator will be able to change the information entered in the Alarm Acknowledgment window.

Alarm description format

The **Alarm description format** drop-down box controls what is displayed as the alarm description in Alarm Monitoring when a generic event is received. This field only applies to generic events. Choices include:

- **Event Text Only -** displays the first line of the event text as the alarm description in Alarm Monitoring. This is the default
- **Alarm Name Only -** displays the alarm name as the alarm description in Alarm Monitoring.
- **Alarm Name** - Event Text: displays both the alarm name and event text as the alarm description in Alarm Monitoring.
- **Event Text** - Alarm Name: displays both the event text and alarm name as the alarm description in Alarm Monitoring.

Alarm description

(view mode only) Lists currently defined alarms, and the type (alarm category) and priority of each alarm.

Name

Indicates the alarm's name. This is the name that will appear in the listing window. Note that some names seem to go together. For example, “Door Held Open” and “Door Held Open Canceled”. These are, respectively, an *initiating alarm* and a *canceling alarm*. Some options selected on this

form affect these paired alarms, as noted in this field table. You can also use this form to create custom alarms with more distinctive or eye-catching names such as “Unauthorized Access - President’s Office”.

Priority

Indicates a priority level for this alarm. You can choose a value in the range of 0 through 255. The priority is highlighted (reverse video) in the color assigned to the value, as specified on the Priority form of this folder. You can view priority assignments and colors for alarms by clicking on the Priority column heading in the alarm description field on this form. This sorts the entries in priority order.

Assigned Event(s)

Lists all event-hardware assignments for the current alarm. Each entry is preceded by an icon, and includes the name of the event, name of the specific hardware device, and the device type.

Link Summary

(displayed only in view mode) Displays the Link Summary View window, which lists all currently defined event-hardware-alarm assignments.

Hardware Devices

(displayed only in modify mode) Lists currently defined hardware devices by name and device type. The icon that precedes each entry indicates the device type, as follows:

access panel

alarm panel

alarm input or reader auxiliary input

alarm output or reader auxiliary output

reader

Access Control Events

(displayed only in modify mode) Lists all currently defined events by name and event type. An icon precedes each entry.

Event text

(displayed only if the Invalid Badge event is selected.) Used to specify event text that is used for an invalid badge event. To use this feature it must be enabled on the General Cardholder Options form. For more information, refer to the Cardholder Options form in the Cardholder Options Folder on page 423.

Event Parameters

(displayed only in modify mode for parameter-based events) Lists all currently defined event parameters by description and parameter number. An icon precedes each entry.

(displayed only in modify mode) Used to assign device-event pairs to the current alarm. The pairs are added to the Assigned Event(s) window.

(displayed only in modify mode) Used to remove device-event assignments from the current alarm. The pairs are removed from the Assigned Event(s) window.

Add
Used to add a custom alarm.

Modify
Used to change an Alarm Description entry.

Delete
Used to remove an Alarm Description entry.

Help
Displays online assistance for this form.

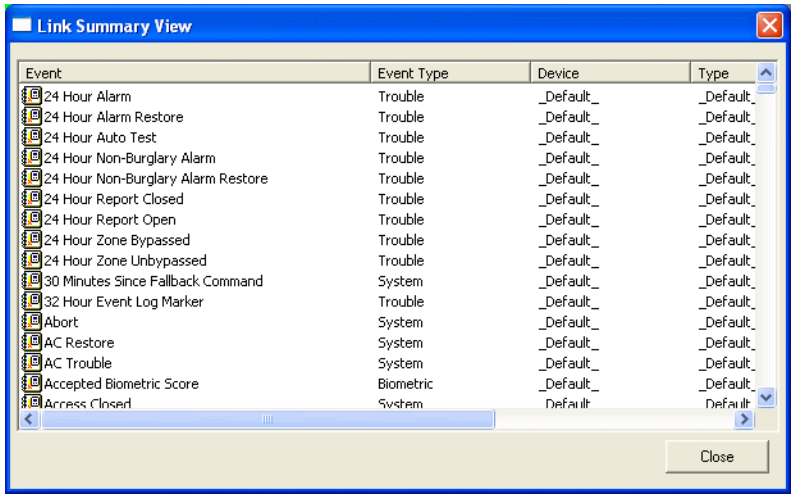
Close
Closes the Alarm Configuration folder.

Alarm Definitions Form Procedures

For more information please refer to Appendix B: Alarm/Event Descriptions on page 1265.

View Device-Event-Alarm Links

The Assigned Events window shows you the device-event assignments for the currently selected alarm only. You can also display a list of ALL hardware device-event assignments for ALL alarm records by clicking on [Link Summary]. This opens the Link Summary View window.



Each row describes one Assigned Event for a specific alarm, with information arranged in the following columns:

- **Event** - event name
- **Event Type** - event category

- **Hardware Name** - device name (or “Default” for a default system alarm’s **Assigned Event**)
- **Type** - device type (or “Default” for a default system alarm’s **Assigned Event**)
- **Alarm** - the alarm to which the device-event pair is assigned

Note: “Default” device types can now be used for custom alarms. In previous versions of OnGuard you were not allowed to create new custom alarms with the “Default” device because it would be duplicating the default alarms that are already in the system. Now with the addition of event parameters you are able to create custom alarms using the “Default” device types.

Click on a column heading to sort the window’s contents by that column. This gives you the flexibility to obtain information such as:

- For a specific event (“Cabinet Tamper”, for example) you can find out which alarms will be triggered.
- For a specific piece of hardware (“Vault Motion Detector”, for example) you can find out which alarms have been created.

Generic Events

The Generic Event event conveys no information other than to indicate that an event has occurred. Once you modify the Generic Event event to run after a certain alarm is triggered you can create a text entry to match the action. For example you could create a Generic Event event for a fire alarm on the first floor of your building. You could then create a text entry “Fire alarm - First floor.”

When creating a Generic Event event you are presented with a drop-down list with your text entries. You select the “Fire alarm - First floor” and that becomes the Generic Events event text. Once that Generic Event is triggered the event text is matched to the text library. If a match is found, the alarm specified with that event text is shown in Alarm Monitoring.

For more information, refer to Chapter 22: Text Library Folder on page 497.

Parameter-Based Events

The Alarm Definitions form also allows you to configure custom alarms for parameter-based events. Examples of devices that use parameter-based events include the Pyrotronics Fire panel, and the Visonic SpiderAlert hardware.

“Trouble In”, “Trouble Out” and “Trouble Acknowledge” are parameter-based events for Pyrotronics Fire panels. Currently all of the Pyrotronics parameters are pre-defined in the OnGuard database and cannot be modified. For more information, refer to Chapter 52: Fire Panels Folder on page 1049.

“Intercom Function” is a parameter-based event for intercoms. For more information, refer to Intercom Functions Form on page 1069.

“Verified” is a parameter-based event for Visonic SpiderAlert transmitters that indicates if the event was received by an infra-red receiver.

Add a Custom Alarm

Note: “Default” device types can now be used for custom alarms. In previous versions of OnGuard you were not allowed to create new custom alarms with the “Default” device because it would be duplicating the default alarms that are already in the system. Now with the addition of event parameters you are able to create custom alarms using the “Default” device types.

1. In the ***Monitoring*** menu, select ***Alarms***. The Alarm Definitions folder opens.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for this alarm.
4. In the **Priority** field, choose a priority to assign to this alarm. The lowest priority that can be assigned is 0, the highest is 255.
5. Below the **Priority** field, select the check box(es) that indicate how you want the alarm to be presented to an Alarm Monitoring station user.

Note: The **Alarm description format** drop-down list applies to generic events only.

6. To assign a device-event linked pair to this alarm:
   a. Select the name of the device in the Hardware Devices window. If you wish to link more than one device to the same event, you can select all those devices in this step.
   b. In the Access Control Events window, select the event you wish to link to the selected device(s).
      - If the event you selected is parameter-based, the Access Control Events window will get smaller, and the **Event Parameters** display field will appear below it. The Alarm Definitions form (modify mode for parameter-based events) illustration demonstrates this.
        In the **Event Parameters** display field, select the event parameter you want to be linked with the device-event linked pair.
      - If the event you selected was the Generic Event, then select the event text in the **Event text** drop-down list.
7. Click on the assign button, . The Assigned Event(s) window will display one entry for the hardware device-event pair you selected. If you selected multiple devices for this event, each will have its own entry.
8. Repeat steps 6 and 7 for each additional event you want to assign to this alarm.
9. To remove one or more device-event assignments from this alarm, select the device-event entry (or entries) in the Assigned Events window, then click on the remove button, . The entry will be removed from the Assigned Events window.

Notes: You cannot remove any of the **Assigned Events** from default system alarms, which are included in the database at the time of installation. If you attempt to delete such an alarm, the following message will be displayed:

"This default assignment is a system default. You cannot remove it!"

You cannot remove all of an alarm's assigned device-events (even if it's a custom alarm). An alarm must have at least one entry in the Assigned Events window.

10. Click [OK].

Modify an Alarm Definition Record

1. In the ***Monitoring*** menu, select ***Alarms***. The Alarm Definitions folder opens.
2. In the alarm description window, select the name of the alarm entry you wish to change.
3. Click [Modify].
4. Make the changes you want to the fields.

Note: The **Alarm description format** drop-down list can be modified for generic events only.

5. Click [OK].

Delete an Alarm Definition Record

1. In the ***Monitoring*** menu, select ***Alarms***. The Alarm Definitions folder opens.
2. In the alarm description window, select the name of the alarm entry you wish to delete.
3. Click [Delete].

Notes: You cannot delete any of the default system alarms, which are included in the database at the time of installation. If you attempt to delete such an alarm, the following message will be displayed:

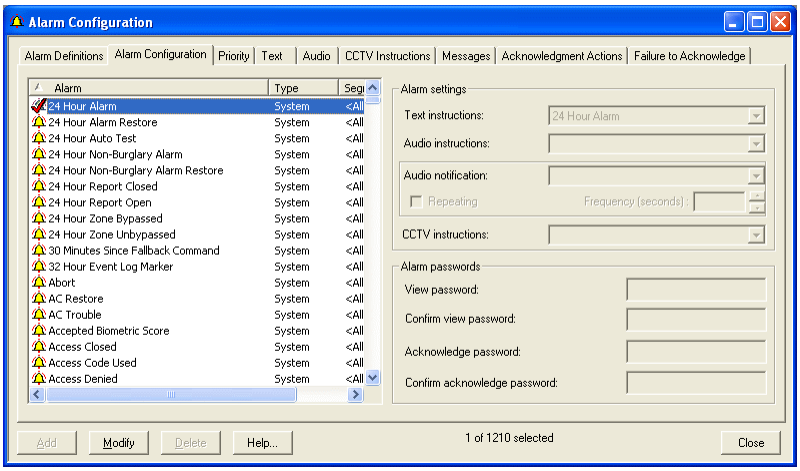
"This is a system entry that cannot be deleted!"

4. Click [OK].
5. Click [Yes] when prompted to proceed with the deletion.

Alarm Configuration Form

This form is used to:

- Password-protect alarm display and acknowledgment
- For a particular alarm, specify text, sound, and camera instructions for monitoring purposes



Text instructions

Indicates the text instructions that will be provided to the monitoring stations when this alarm occurs. Choices include the names of all currently defined text instruction records, defined on the Text form. For this reason, only Text records that have "Instruction" selected in the **Type** field will be listed here.

Audio instructions

Audio instructions are played when the Audio button in the Acknowledgement dialog is selected. Choices include the names of all currently defined audio instruction records, defined on the Audio form. For this reason, only Audio records having the **Instruction** radio button selected will be listed here.

Audio notification

Selects the audio announcement that will be made at the monitoring stations when this alarm occurs. Choices include the names of all currently defined audio notification records, defined on the Audio form. For this reason, only Audio records having the **Notification** radio button selected will be listed here. The audio notification will play once unless the **Repeating** check box is selected.

Repeating

Available only if an audio notification is selected from the **Audio notification** drop-down list. If selected: when the alarm occurs, the audio notification will play over and over again at an interval specified by the **Frequency (seconds)** field. At a given monitoring station, the notification will continue to play until either the alarm is acknowledged or it is deleted from that station. If not selected: the audio notification will play once.

Frequency (seconds)

Available only if the **Repeating** check box is selected. Specifies the frequency, in seconds, with which an audio notification will be repeated.

CCTV instructions

Indicates the instructions that will be provided to the CCTV equipment when this alarm occurs. Choices include the names of all currently defined CCTV instruction records, defined on the CCTV Instructions form. The instructions are sent to the CCTV controller that is attached to the monitoring workstation (as configured on the Workstations form in the System Configuration folder).

Alarm passwords

You can use passwords to restrict the ability to view and acknowledge specific alarms. This section includes the View Password, Confirm View Password, Acknowledge Password, and Confirm Acknowledge Password fields.

View password

Type a password here if you wish to require a password to be able to view the Alarm Acknowledgment window for this alarm on an Alarm Monitoring station. You can use up to 32 characters, including letters and numbers. This field is case-sensitive: it distinguishes upper- from lowercase letters. For example, “SECURITY”, “security”, and “SecuRitY” are considered to be three different words. If a password is entered here, you must enter EXACTLY the same password in the **Confirm view password** field.

Confirm view password

If a password was entered in the **View password** field, you must enter EXACTLY the same password here.

Acknowledge password

Type a password here if you wish to require a password to be able to acknowledge this alarm from an Alarm Monitoring station. You can use up to 32 characters, including letters and numbers. Like View Password, this field is case-sensitive. If a password is entered here, you must enter EXACTLY the same password in the **Confirm acknowledge password** field.

Confirm acknowledge password

If a password was entered in the **Acknowledge password** field, you must enter EXACTLY the same password here.

Alarm description
Lists currently defined alarms and the type (alarm category) for each.

Alarm Settings
Includes the Text Instructions, Audio Instructions, Audio Notification, Repeating, Frequency (sec), and CCTV Instructions fields.

Modify
Used to change an alarm's configuration.

Help
Displays online assistance for this form.

Close
Closes the Alarm Configuration folder.

Alarm Configuration Form Procedures

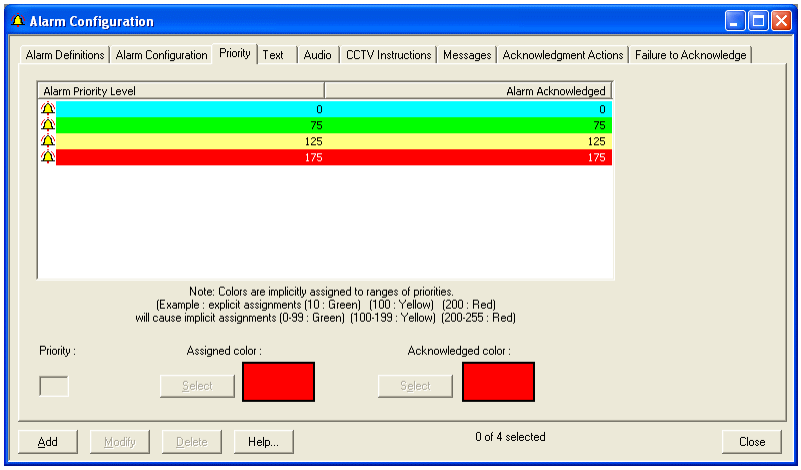
The following procedures can be performed on this form.

Configure an Alarm

1. Click [Modify].
2. In the alarm description window, select the entry you wish to configure.
3. In the Alarm Settings section, choose the text instructions, audio announcement and instructions, and CCTV instructions for this alarm.
4. If you want to restrict the ability to view this alarm, complete the **View Password** and **Confirm View Password** fields.
5. If you want to restrict the ability to acknowledge this alarm, complete the **Acknowledge Password** and **Confirm Acknowledge Password** fields.
6. Click [OK].
   - When the selected alarm occurs, the selected audio notification will be announced at the Alarm Monitoring stations, and the selected CCTV command will be sent to your CCTV system for action. The selected audio and text instructions will be available to assist the monitoring station users.

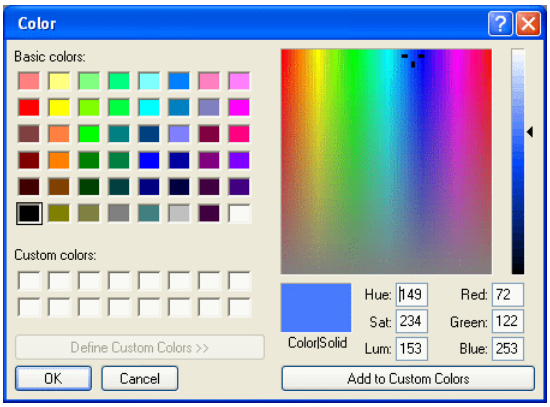
Priority Form

This form is used to configure colors to be associated with alarm priority ranges.



Color Form

This form is opened by clicking on either of the [Select] buttons on the Priority form.



Alarm Priority Level

Lists all currently defined alarm priority colors and their minimum values.

Priority

Specifies the minimum value in the range of priorities that will be displayed in the **Assigned color**. By indicating a **Priority** you are actually defining a range of values that starts with the number you specify and ends just before the first number of the next priority range. This is illustrated by the default values, which are:

- Green alarms have a **Priority** value 0; actual range is 0 - 84
- Yellow alarms have a **Priority** value 85; actual range is 85 - 169
- Red alarms have a **Priority** value 170; actual range is 170 - 255

Alarms can have priorities in the range of 0 through 255. Because all of those values display in some color, a **Priority** you specify may be adjusted to 0. For example, specifying:

pink = 25, blue = 100, yellow = 150, black = 200

will result in the following ranges: pink (0 - 99), blue (100 - 149), yellow (150 - 199), and black (200 - 255)

Assigned color
Displays the selected color assigned to the specified **Priority**

Select
Opens the Color form, from which you can select a color for the **Assigned color** field.

Acknowledged color
Displays the selected color assigned to the acknowledged alarm of the specified **Priority**.

Select
Opens the Color form, from which you can select a color for the **Acknowledged color** field.

Add
Used to add a color for a range of alarm priorities.

Modify
Used to change the color assigned to a range of alarm priorities.

Delete
Used to delete the color assigned to a range of alarm priorities.

Help
Displays online assistance for this form.

Close
Closes the Alarm Configuration folder.

Priority Form Procedures

You may choose to accept the default alarm priority ranges and their assigned colors. Or you can modify their colors and/or values. Alternatively, you can add or remove priority ranges as appropriate for your environment.

Define an Alarm Priority Range

1. Click [Add].
2. In the **Priority** field, type a number that's in the range of 0 through 255. Remember that this number specifies the minimum in range that's limited by the next higher color.
3. Click the [Select] button next to the **Assigned Color** display.
4. On the Color form, do one of the following:
   a. select one of the Basic Colors by clicking on it
   b. click [Define Custom Colors >>] to expand the window. Then:
      - click on the color palette to select a precise color, or
      - specify the color by entering red, green, blue, hue, saturation, and luminance values
5. Click [OK] to close the Color form. The selected color will be displayed in the **Assigned Color** field.
6. Click the [Select] button next to the **Acknowledged Color** display, then repeat step 4.
7. Click [OK] to close the Color form. The selected color will be displayed in the Acknowledged Color field.

8. Click [OK].

Modify an Alarm Priority Range

1. In the **Alarm Priority Level** field, select the priority range to be modified.
2. Click [Modify].
3. Make your desired changes.
4. Click [OK].

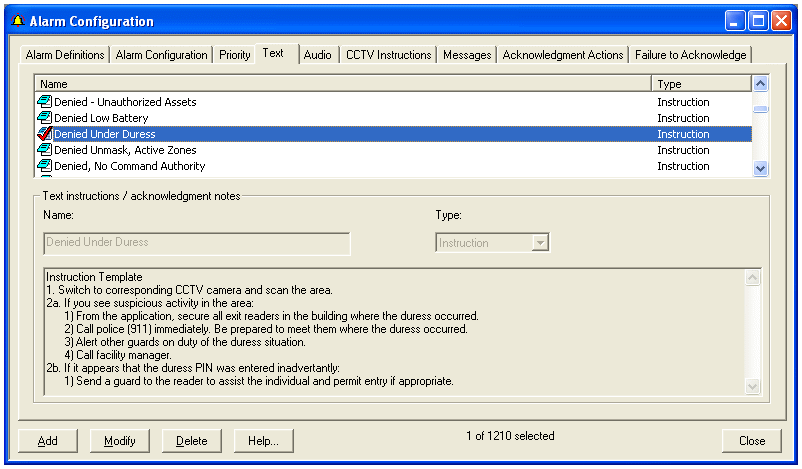
Delete an Alarm Priority Range

1. In the **Alarm Priority Level** field, select the priority range to be deleted.
2. Click [Delete].
3. Click [OK].

Text Form

This form is used to:

- Write the text instructions that will be displayed on an Alarm Monitoring station when a specific alarm occurs.
- Preconfigure information to be placed in the **Notes** field during alarm acknowledgment.



Listing window

Lists the names of currently defined text records, and the type (instruction or acknowledgment note) for each.

Text instructions/ acknowledgment notes

Includes the **Name** and **Type** fields and the instructions window.

Name

Indicates the name of the text record.

Type
Indicate the type of text record you are defining. Choices include:

- Instruction - if selected, the text in the edit window will be displayed on an Alarm Monitoring station when a particular alarm is viewed.
- Ack. Note - if selected, the text in the edit window will be available for use during alarm acknowledgment. An Alarm Monitoring station user can click [Select Notes] in the Alarm Acknowledgment window and select this record, thereby inserting the text into the **Notes** field of the Alarm Acknowledgment window.

Instructions window
Contains the actual text information (up to 32,000 characters) that will be displayed in the Alarm Monitoring application when a specific event is triggered. The window will expand to accommodate whatever you type (up to 32,000 characters).

Add
Used to add a text record.

Modify
Used to change a text record.

Delete
Used to remove a text record.

Help
Displays online assistance for this form.

Close
Closes the Alarm Configuration folder.

Text Form Procedures

The following procedures can be performed on this form.

Add a Text Record

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for this text record.
3. In the **Type** field, choose whether this information will be used for instruction in response to an alarm, or for notes during alarm acknowledgment.
4. In the edit window, type the actual text information as you wish it to be displayed on an Alarm Monitoring workstation. The window will expand to accommodate whatever you type (up to 32,000 characters).
5. Click [OK].

Modify a Text Record

1. In the listing window, select the name of the text record you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.

4. Click [OK].

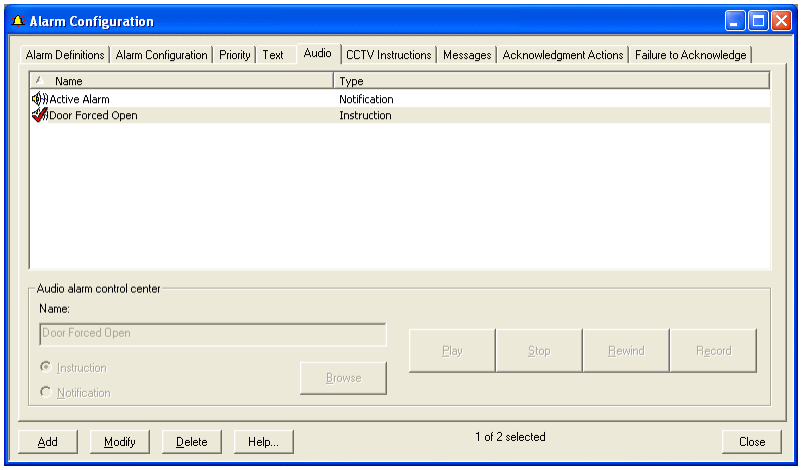
Delete a Text Record

1. In the listing window, select the name of the text record you wish to delete.
2. Click [Delete].
3. Click [OK].
4. Click [Yes] when prompted to proceed with the deletion.

Audio Form

This form is used to import or record an audio clip to be played on an Alarm Monitoring station when a specific alarm occurs. The clip can be used as either of the following:

- An audible announcement when the alarm is triggered.
- Verbal instructions for responding to the alarm.



listing window

Lists the names of currently defined audio clips, and each one's type.

Name

Indicates the name of the audio clip.

Instruction

An audio clip can be used either to announce the arrival of an alarm, or to instruct a monitoring station user how to respond to the alarm. Select this radio button if this audio clip is to be used for instruction.

Notification

An audio clip can be used either to announce the arrival of an alarm, or to instruct a monitoring station user how to respond to the alarm. Select this radio button if this audio clip is to be used to announce the alarm's arrival.

If you do not have the ability to record audio on your computer, or if your organization has not purchased the Custom Voice Alarm option, you can still select this radio button. In such situations, a standard beep will be played through the computer speaker at the Alarm Monitoring stations.

Like custom notifications, the standard beep will repeat at regular intervals if the **Repeating** check box has been selected for this alarm on the Alarm Configuration form.

Browse

If you do not wish to record audio clips from within the software, you can import existing audio files to use for alarm notification and instruction.

This button opens an Open form, from which you can select a standard Wave (*.WAV) format audio file to import.

Play

Plays an audio clip once from beginning to end.

Stop

Stops an audio clip Record or Play operation.

Rewind

Rewinds an audio clip to its beginning.

Record

Records an audio clip.

Add

Used to add an audio clip record.

Modify

Used to change an audio clip record.

Delete

Used to remove an audio clip record.

Help

Displays online assistance for this form.

Close

Closes the Alarm Configuration folder.

Audio Form Procedures

The following procedures can be performed on this form.

Add an Audio Clip Record

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for this audio clip record.
3. Specify whether this clip is to be used for **Instruction** or **Notification**.
4. Do one of the following:
   a. Use the [Browse] button to import an existing audio file
   b. Use the following buttons to create your own audio clip from within the application (your computer must be equipped to record audio):

- [Record] starts recording the audio clip
- [Play] plays the audio clip
- [Stop] stops the audio clip recording or playback operation
- [Rewind] rewinds the audio clip to its beginning

5. Click [OK].

Modify an Audio Clip Record

1. In the listing window, select the name of the audio clip record you wish to change.
2. Click [Modify].
3. Make the changes you want to the record.
4. Click [OK].

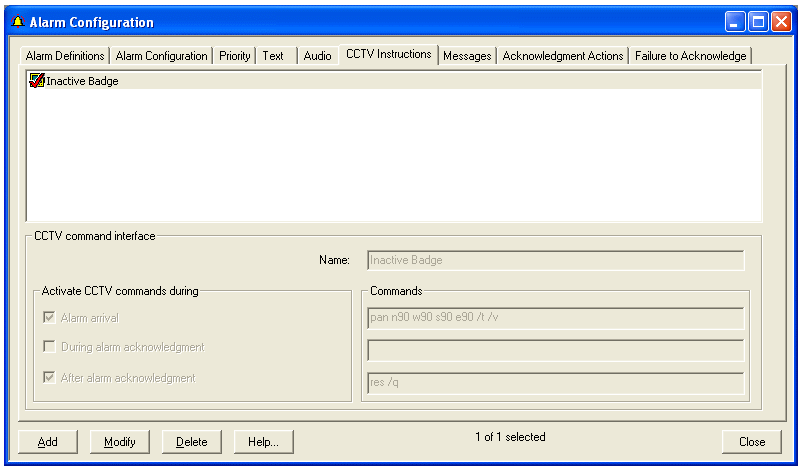
Delete an Audio Clip Record

1. In the listing window, select the name of the audio clip record you wish to delete.
2. Click [Delete].
3. Click [OK].
4. Click [Yes] to confirm deletion.

CCTV Instructions Form

This form is used to store the commands that will be communicated to your CCTV device in response to a specific alarm event.

Note: The CCTV instructions you configure are automatically sent to the CCTV controller attached to the monitoring station when that station receives the alarm. The CCTV controller is configured in the Workstations folder.



listing window

Lists currently defined CCTV instructions.

CCTV command interface
Includes the **Name** field, plus the Activate CCTV Commands During and Commands sections.

Name
Indicates the name of the CCTV instructions.

Activate CCTV commands during
Includes the Alarm Arrival, During Alarm Acknowledgment, and After Alarm Acknowledgment fields.

Alarm arrival
Select this check box to enter a CCTV command that will be put into effect upon alarm activation.

During alarm acknowledgment
Select this check box to enter a CCTV command that will be in effect during alarm acknowledgment.

After alarm acknowledgment
Select this check box to enter a CCTV command that will be put into effect after alarm acknowledgment.

Commands
Includes three (3) command string text fields.

command string 1
Enter a command string to be sent to your CCTV device upon alarm activation. If your equipment uses control characters as commands, refer to the special note following the procedures in this section.

command string 2
Enter a command string to be sent to your CCTV device during alarm acknowledgment. If your equipment uses control characters as commands, refer to the special note following the procedures in this section.

command string 3
Enter a command string to be sent to your CCTV device after alarm acknowledgment. If your equipment uses control characters as commands, refer to the special note following the procedures in this section.

Add
Used to add CCTV instructions.

Modify
Used to change CCTV instructions.

Delete
Used to remove CCTV instructions.

Help
Displays online assistance for this form.

Close
Closes the Alarm Configuration folder.

CCTV Instructions Form Procedures

The following procedures can be performed on this form.

Add a CCTV Instruction Record

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for this CCTV instruction record.
3. In the Activate CCTV Commands During section, select one of the check boxes, which indicate when to activate the CCTV command.
4. In the Commands section, click in the text field to the right of the selected check box, and type a valid CCTV command string. The command will direct the Closed Circuit Television equipment to perform a specific action, such as to pan a particular area. For specific commands, refer to the user manual that was provided with the CCTV equipment used at your installation. If your equipment uses control characters as commands, refer to the special note following the procedures in this section.
5. Repeat steps 3 and 4 for each additional CCTV command you want to activate when this event occurs. Note that you can have the CCTV camera do one thing when the alarm occurs, do something else while the alarm is being acknowledged, and do a third thing after the alarm has been acknowledged.
6. Click [OK].

Modify a CCTV Instruction Record

1. In the listing window, select the name of the CCTV instruction record you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK].

Delete a CCTV Instruction Record

1. In the listing window, select the name of the CCTV instruction record you wish to delete.
2. Click [Delete].
3. Click [OK].
4. Click [Yes] to confirm that you want the record deleted.

Use Control Characters in CCTV Command Strings

Some CCTV switchers include control characters in their command strings. The following chart lists character sequences that can be entered in a command string to produce the corresponding control character.

Control Character	Character Sequence to Enter
newline (Hex 0A)	\n
tab (Hex 09)	\t
vertical tab (Hex 0B)	\v

Control Character	Character Sequence to Enter
backspace (Hex 08)	\b
carriage return (Hex 0D)	\r
formfeed (Hex 0C)	\f
alert character (Hex 07)	\a
start of header (Hex 01)	\soh
hex character Any character with hex value 0x00 through 0xff can be configured by entering \x followed by two characters representing the hex value. The two hex characters (not one character) must be configured. For example, \x1 will not be converted to a hex value. \x01 must be used in order to specify the character with hex value 0x01. \x is case-sensitive. \X01 will not be converted to a hex value, but \x01 will. The hex characters themselves are not case-sensitive. \xaa and \xAA will both be converted to the character with hex value 0xaa.	\x00 through \xff

IMPORTANT: Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

In order for the Alarm Monitoring system to treat these character sequences as control characters, the following statements need to be included in the ACS.INI file (located in your Windows operating system directory). This should be done on the computer that is connected to the CCTV switching equipment and running the Alarm Monitoring application:

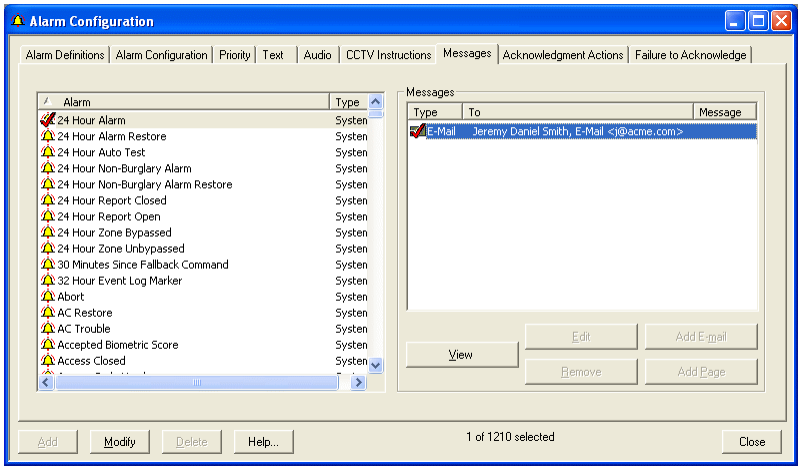
[MONITORING]

CCTV_BACKSLASH_PRECEDES_CONTROL_CHARS=1

Messages Form

This form is used to create e-mail and pager messages and link them to defined alarms. This ensures that specific individuals are automatically informed when the alarms occur.

Note that e-mail recipients must first be configured on the Recipients form in the Global Output Devices folder (The Recipients form is opened by selecting ***Global Output Devices*** from the ***Monitoring*** menu, then clicking on the Recipients tab.)



Alarm

Lists all currently defined alarms, as defined on the Alarm Definitions form.

Messages

Indicates the messages that are currently defined for the selected alarm.

A Type of indicates an E-mail message

A Type of indicates a pager message

View

Displays the recipient(s), subject, and content of the selected message.

Edit

(displayed in modify mode only) Allows you to edit the selected message.

Remove

(displayed in modify mode only) Deletes the selected message.

Add E-mail

(displayed in modify mode only) Click this button to add an automatic e-mail message. Doing so opens the Add E-mail Message window, from which you can select recipients and enter the subject and body text of the message.

Add Page

(displayed in modify mode only) Click this button to add an automatic page message. Doing opens the Add Pager Message window, from which you can select recipients and type the message to be sent.

Add

This button is not used.

Modify

Modifies the message assignments for the selected alarm.

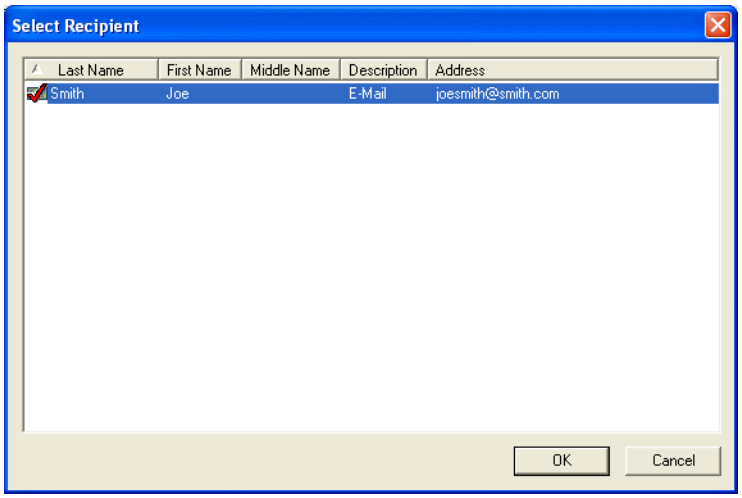
Delete

This button is not used.

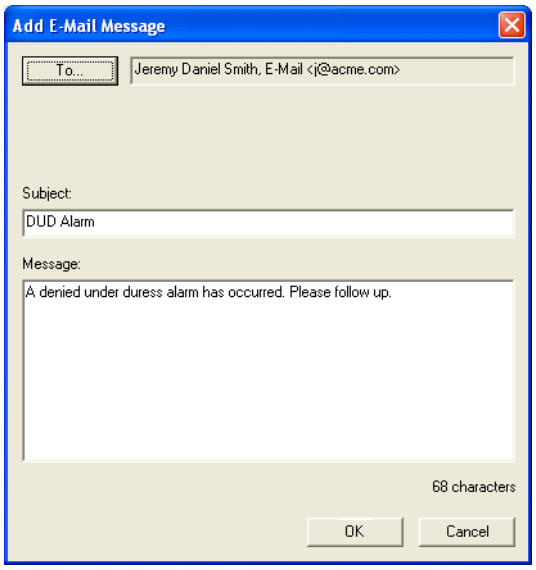
Help
Display online help for this topic.

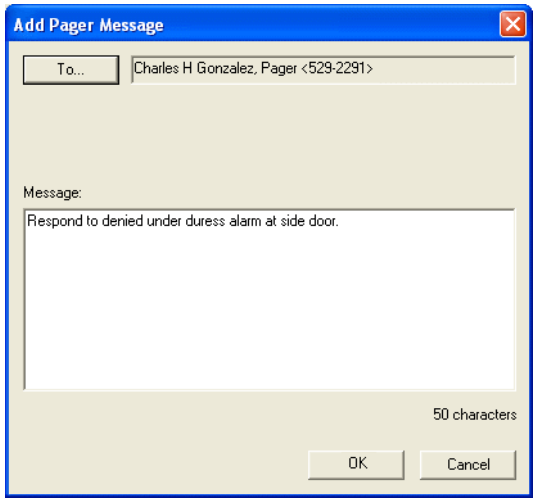
Close
Closes the Alarm Configuration folder.

Select Recipient Window



Add E-mail /Pager Windows





To

Clicking this button opens the Select Recipient window, from which you can select addresses that will receive the message.

Subject

Displayed only on the Add E-Mail Message window. Type a description for the alarm, which will be displayed in the subject line of the message.

Message

Determines what will be displayed in the message. When a Message is being configured, you can specify parameters or “placeholders” for alarm occurrence specific information within the message body. These parameters will be automatically filled in at runtime with the proper message data. This information can include the Alarm Description, Alarm Priority, Time of Alarm Occurrence, Device Name, Badge ID, and/or Cardholder Name. When the Message is configured, the following strings will indicate a parameter to be filled in at runtime:

- **%alarmDescription:** Alarm Description of the Alarm that generated the Message
- **%alarmPriority:** Priority of the Alarm that generated the Message
- **%alarmTime:** Time at which the Alarm generated the Message
- **%deviceName:** Name of the Device associated with the Alarm that generated the Message
- **%badgeID:** Badge ID associated with the Alarm that generated the Message
- **%cardholderName:** Cardholder Name associated with the Alarm that generated the Message

If the message body is left empty/blank, the details pertaining to the Alarm will be automatically filled in and the message sent.

OK

Saves changes and returns you to the Messages form.

Cancel

Cancels pending changes and returns you to the Messages form.

Messages Form Procedures

The following procedures can be performed on this form.

Add an Automatic E-mail Message

Note: The Global Output Server must be running for this to work.

1. Select the alarm for which an automatic message will be created.
2. Click [Modify]. For each e-mail message you wish to send whenever this alarm occurs, perform steps 3-7.
3. Click [Add E-mail] to open the Add E-Mail Message window.
4. To specify message recipient(s), click [To]. This opens the Select Recipient window, which contains a list of all currently defined e-mail recipients. Select one or more recipients by clicking on their icons to place a checkmark on each. Click [OK] when you have selected all intended recipients.

Note: E-mail recipients must first be configured on the Recipients form in the Global Output Devices folder (The Recipients form is opened by selecting ***Global Output Devices*** from the ***Monitoring*** menu, then clicking on the Recipients tab.)

5. Enter the subject of the message. This information will be displayed in the Message column of this entry in the Messages display window on the Messages form.
6. In the Message field, enter the actual content of the message to be sent. Notice that the number of characters contained in the message is displayed in the lower right corner of the window. Refer to the Message entry in the Add E-Mail/Pager Message form field table in this chapter for message configuration details.
7. Click [OK] to save your changes and close the Add E-Mail Message window. Or, click [Cancel] to exit without saving your changes.
8. After you have added all the e-mail messages you want sent in response to the selected alarm, click [OK] on the Messages form.

Add an Automatic Page Message

Note: The Global Output Server must be running for this to work.

1. Select the alarm for which an automatic message will be created.
2. Click [Modify]. For each pager message you wish to send whenever this alarm occurs, perform steps 3-6.
3. Click [Add Page] to open the Add Pager Message window.
4. To specify message recipient(s), click [To]. This opens the Select Recipient window, which contains a list of all currently defined paging recipients. Select one or more recipients by clicking on their icons to place a checkmark on each. Click [OK] when you have selected all intended recipients.

Note: Page recipients must first be configured on the Recipients form in the Global Output Devices folder (The Recipients form is opened by selecting ***Global Output Devices*** from the ***Monitoring*** menu, then clicking on the Recipients tab.)

5. In the Message field, enter the actual content of the message to be sent. In the lower right corner of the window, the number of characters in the message will be updated as you type. Refer to the

Message entry in the Add E-Mail/Pager Message form field table in this chapter for message configuration details.

6. Click [OK] to save your changes and close the Add Pager Message window. Or, click [Cancel] to exit without saving your changes.
7. After you have added all the pager messages you want sent in response to the selected alarm, click [OK] on the Messages form.

View an Automatic Message

1. In the Alarm display window, select the alarm you'd like to view messages for.
2. In the Message display window, select the message you would like to view.
3. Click [View] to display message contents in the corresponding View Message window.

Modify an Automatic Message

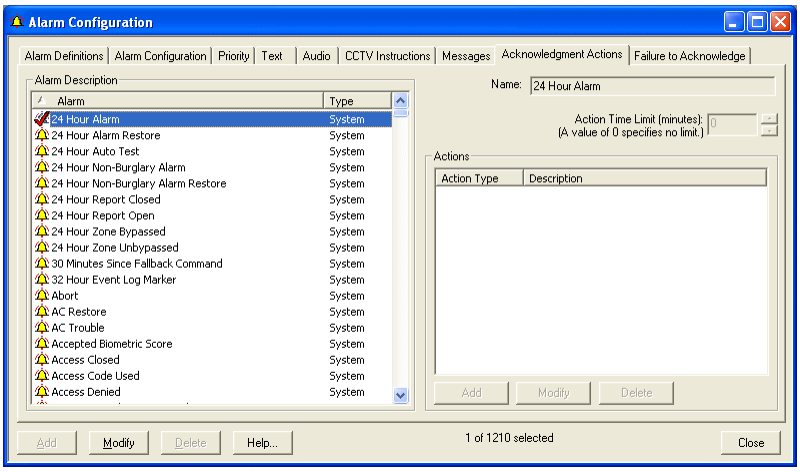
1. Select the alarm for the message you'd like to change.
2. Click [Modify].
3. Select the message you wish to change.
4. Click [Edit].
5. Make the desired changes to the recipient list, subject, and/or message body.
6. Click [OK] to save your changes and close the Edit Message window.
7. Click [OK] on the Messages form to save your changes, or [Cancel] to lose them.

Delete an Automatic Message

1. Select the alarm for the message you'd like to change.
2. Click [Modify].
3. Select the message you would like to delete.
4. Click [Remove]. The message is removed from the Messages display window. However, the message is not actually deleted until you complete step 5.
5. Click [OK] on the Messages form to delete the selected message. If you do not wish to delete the selected message, click [Cancel] to restore the message to the Messages display window.

Acknowledgment Actions Form

Acknowledgment actions are commands that are automatically executed by Alarm Monitoring when an alarm is acknowledged. This form is used to configure acknowledgment actions to execute OnGuard actions. For example, you can configure an acknowledgment action to automatically execute a function list (an action) when a particular alarm is acknowledged.



Alarm

Lists all currently defined alarms, as defined on the Alarm Definitions form.

Name

Indicates the name of the selected alarm.

Action Time Limit (minutes)

Specifies the length of time after which, if the alarm hasn't been acknowledged, the action won't be executed. A value of 0 specifies no limit.

Actions

Contains the Action Type/Description listing window, and the [Add], [Modify], and [Delete] push buttons.

Action Type/Description listing window

Displays a list of all currently configured actions.

Add

Click this button to open the Add Action Wizard from where you can add an action.

Modify

Click this button to modify an existing alarm acknowledgment action.

Delete

Click this button to delete an existing alarm acknowledgment action.

Modify

Click this button to assign an action to an alarm.

Help

Displays online assistance for this form.

Close

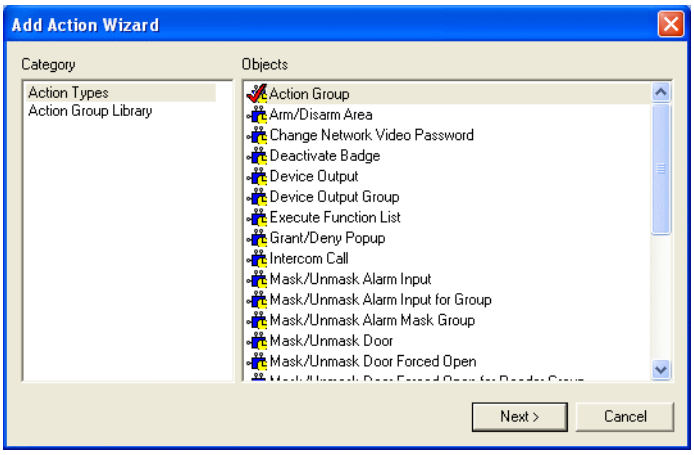
Click this button to close the Alarm Configuration folder.

Acknowledgment Actions Form Procedures

The following procedures can be performed on this form.

Configure Acknowledgment Actions

1. Select ***Alarms*** from the ***Monitoring*** menu. The Alarm Configuration folder opens.
2. Click the Acknowledgment Actions tab.
3. Select an alarm from the listing window. The name of the alarm you select will be displayed in the **Name** field.
4. Click [Modify].
5. In the Actions section, click [Add]. The Add Action Wizard opens.



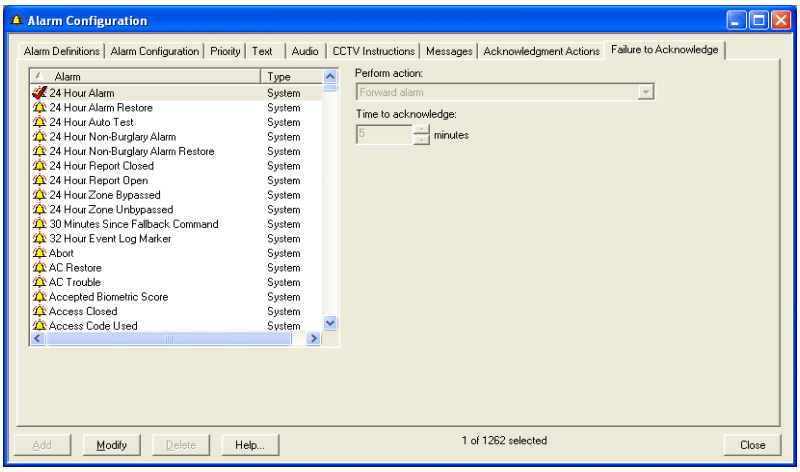
6. Choose an action **Category**, and then select an action **Object**.
7. Click [Next]. Depending on which Category/Object combination you chose in step 6, a corresponding action properties window will open.
8. Configure the action you selected in step 6. To do this, you must refer to the Actions appendix for information on each action properties window. For more information please refer to Appendix A: Actions on page 1193.
9. The action you just added will be displayed in the Action Type/Description listing window. Repeat steps 5-8 for each action that you want to assign to the selected alarm.
10. Click [OK].

Failure to Acknowledge Form

The Failure to Acknowledge action allows you to define if alarms that are not acknowledged in a set number of minutes should be forwarded or highlighted in Alarm Monitoring. This form is used to configure such actions. For example, you can configure a failure to acknowledge action to automatically highlight an alarm that was not acknowledged after five minutes of happening.

If the alarm is configured to highlight, and it has not been acknowledged within the time-frame specified, an “Alarms waiting to be acknowledged” popup will appear in alarm monitoring.

If an alarm is forwarded to another station a blue arrow will appear next to it in the alarm list. If it was forwarded from another station a green arrow will appear next to it. A broken red arrow will appear if the forward failed.



Alarm

Lists all currently defined alarms, as defined on the Alarm Definitions form.

Perform action

Allows you to select:

- **None** - No action will be taken
- **Forward alarm** - The alarm will be forwarded if it is not answered in the set number of minutes.
- **Highlight alarm** - The alarm will be highlighted if it is not answered in the set number of minutes.

Time to acknowledge

Specifies the length of time after which, if the alarm hasn't been acknowledged, that the action chosen in the **Perform action** drop-down box will occur.

Failure to Acknowledge Form Procedures

The following procedures can be performed on this form.

Configure a Failure to Acknowledge Action

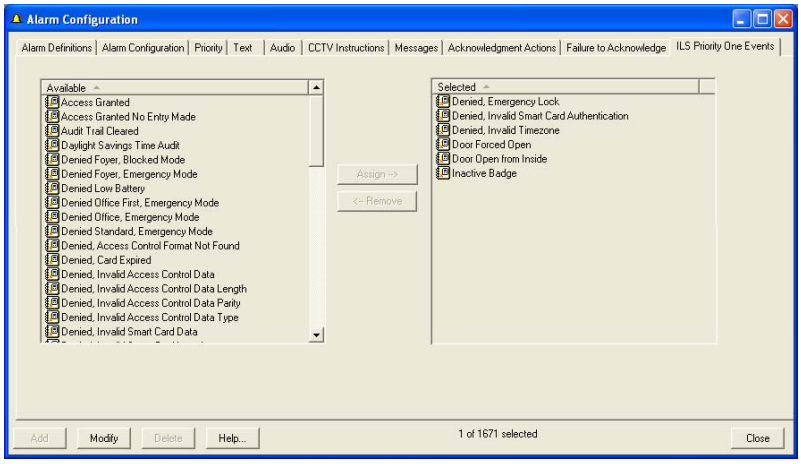
1. In the **Alarm** list box, choose the alarm you wish to configure for a failure to acknowledge action.
2. Click [Modify].
3. In the **Perform action** drop-down, select the action you wish to take place.
4. In the **Time to acknowledge** scroll box, set the number of minutes that the alarm must go unacknowledged before the failure to acknowledge action occurs.
5. Click [OK].

ILS Priority One Events Form

Note: To view this form your system must have an ILS license.

Use this form to specify up to 20 ILS wireless lock events as priority one events on a system-wide. By default, all ILS wireless locks are configured with the system priority one events.

To configure priority one events on a lock-by-lock basis, use the ILS Priority One Events form in the Readers folder.



Available

Lists all ILS wireless lock events.

Selected

Lists ILS wireless lock events assigned as priority one events. Priority one events are sent to Alarm Monitoring, filtering out all other lock events.

Assign

Click to move selected events to the list of priority one events. Up to 20 events can be assigned as priority one.

Remove

Click to remove events from the list of priority one events.

Modify

Used to change an event's configuration.

Help

Displays online assistance for this form.

Close

Closes the ILS Priority One Events form.

ILS Priority One Events Form Procedures

To read how to configure an ILS locking system, refer to Appendix K: Lenel ILS (Integrated Locking Solutions) on page 1473..

CHAPTER 44

Monitor Zones Folder

The Monitor Zones folder contains forms with which you can:

- Define monitor zones, and specify which device(s) are to be included in each
- Choose the workstations that will be able to monitor the selected monitor zone
- Choose the intercom station that the workstation will place calls from
- Define event routing groups
- Assign one or more events to a particular group
- Assign (event + timezone) pairs to an event routing group
- Link monitoring zones with action groups

The folder contains three forms: the Monitor Zones form, the Monitor Stations form, and the Event Routing form.

The Monitor Zones folder is displayed by selecting ***Monitor Zones*** from the ***Monitoring*** menu or by selecting the Monitor Zones toolbar button.

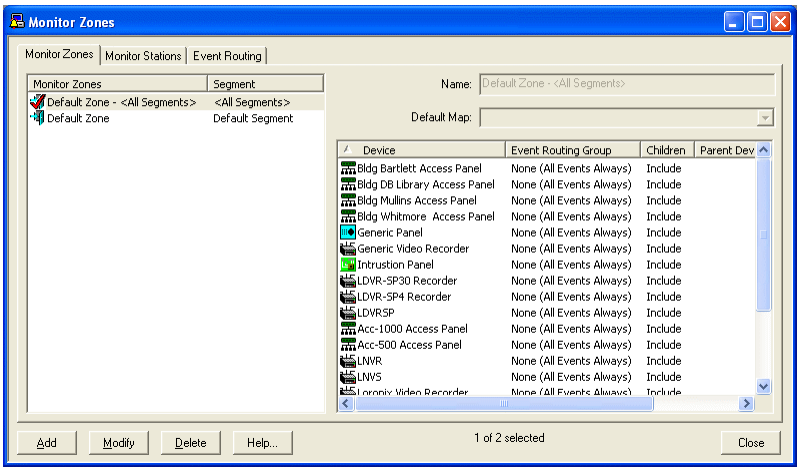
Toolbar Shortcut

Note: For users of segmentation, Monitor Zones can now belong to a Segment group, instead of just <All Segments> or one segment. This allows a monitor zone to contain hardware from all segments in the segment group. For more information please refer to Appendix E: Segmentation on page 1411.

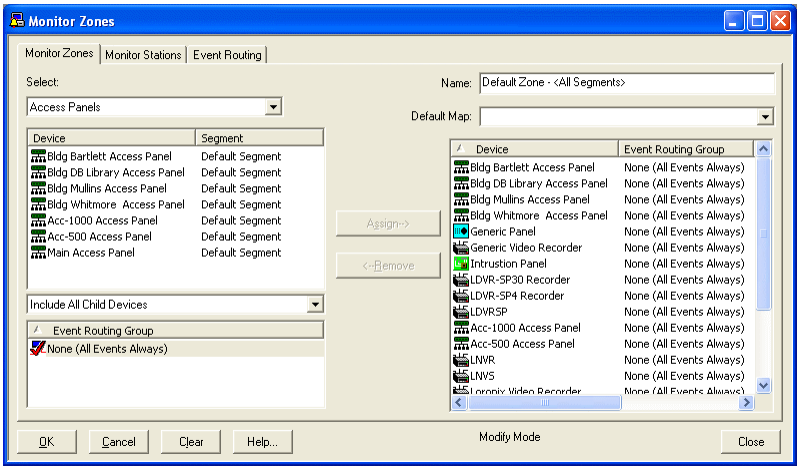
Monitor Zones Form

This form is used to create monitor zones, assign a map to a monitor zone, and specify devices (and optionally, event routing groups) to be included in a zone.

Monitor Zones Form (View Mode)



Monitor Zones Form (Modify Mode)



Monitor Zones

(view mode only) Lists currently defined monitor zones. If your installation uses segmentation, the assigned segment is also indicated here.

Name

Specifies the name of the monitor zone.

Default Map

Lists the names of all maps stored in the database. A monitor station can be associated with multiple monitor zones, each of which can have one associated map. Maps are created using MapDesigner.

Event Routing Groups

(modify mode only) Lists all existing event routing groups, as defined on the Event Routing form of this folder.

Assignment window

Lists all (device + event routing group) pairs currently defined for the current monitor zone. Each entry contains the following components:

– Device - the name of the device, preceded by the appropriate icon for that device type

- Event Routing Group - the name of the event routing group
- Children - how the indicated Device's children are handled by this monitor zone. This value is either **Include**, if "Include All Child Devices" was selected from the **child** drop-down list; or **Specify**, if "Specify Child Devices Individually" was selected from the **child** drop-down list.
- Parent Device - the name of the parent device for the indicated Device. If the device is an access panel, it has no parent device. If the device is an alarm panel or reader, its parent is the access panel to which it is attached. If the device is an alarm input or alarm output, its parent is the alarm panel.

Note that if the device is a video recorder, it has no parent device. If the device is a camera, its parent is the video recorder to which it is attached.

If your installation uses segmentation, the assigned segment is also indicated here.

Select

(modify mode only) Selects the type of device to be displayed in the device window when assigning device-event routing group pairs to a monitor zone. Choices include Access Panels, Action Groups, Readers, Reader Inputs, Reader Outputs, Alarm Panels, Alarm Inputs, Alarm Outputs, Video Recorders, Cameras, Monitors, Fire Panels, Intercom Exchanges, Intercom Stations, and Personal Safety Panels.

device window

(modify mode only) Lists all currently defined devices of the type selected from the **Select** drop-down list. Based on that type, only those devices that can be assigned to the monitor zone will be displayed. For example, if you select "Readers" in the **Select** drop-down list, only readers for access panels that are in the monitor zone and are configured for specifying children devices individually will be displayed in the device window. If the device has a parent, the parent device is also listed. Each entry is preceded by the appropriate icon.

Child

(modify mode only) Indicates how the children of the selected device(s) are handled by this monitor zone. Choice include:

- Include All Child Devices - all child devices of the selected access panel, alarm panel, video recorder, or camera will be assigned to this monitor zone
- Specify Child Devices Individually - if selected, you will be able to assign each child device individually to a monitor zone

This field is activated only if you have selected Video Recorders, Fire Panels, Intercom Exchanges, Personal Safety Panels from the **Select** drop-down list. For all other device types, this field is dimmed but displays the "Include All Child Devices" value.

Children devices can only be added to the Monitor Zone if their parent is already assigned to the Monitor Zone.

Assign

(modify mode only) Assigns the selected device(s), event routing group, and child value to the current monitor zone.

Remove

(modify mode only) Removes the selected device from the current monitor zone.

Add

Used to add a monitor zone entry.

Modify
Used to change a monitor zone entry.

Delete
Used to remove a monitor zone entry.

Help
Displays online assistance for this form.

Mode
In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close
Closes the Monitor Zones folder.

Monitor Zones Form Procedures

Use the following procedures on this form.

Add a Monitor Zone

1. Click [Add].
2. In the **Name** field, type a unique, descriptive name for the monitor zone.
3. In the **Select** field, choose what device type to display in the Device window.
4. In the Device window list, select one or more device(s) to be contained in the monitor zone. To select a device you must click on the icon that precedes it.
5. If a device can have children devices, select whether to **Include All Child Devices** or **Specify Child Devices Individually**.
6. If you want to associate an event routing group with these devices (it's not required), select it in the Event Routing Groups list. If you selected more than one device in step 4, each of them will be assigned to this event routing group.

Note: Event Routing Groups are defined on the Event Routing form of this folder.

7. Click [Assign]. This inserts the selected (device + event routing group) pairs into the assignment window.
8. Repeat steps 2-7 as needed to add more devices to the zone.
9. In the Default Map list, select the name of a map to assign as the default map for the monitor zone. Choose a map that represents the physical area that is covered by the selected devices.
10. Click [OK]. The name of the zone will be inserted alphabetically into the Monitor Zones list. You assign workstations to monitoring zones using the Monitor Stations form of this folder. Each such workstation will then be able to monitor the alarm events that occur at hardware devices included in that zone.

Modify a Monitor Zone

1. Select the name of the monitor zone in the Monitor Zones list. The assignment window will list the devices and event routing groups that are included in the zone.

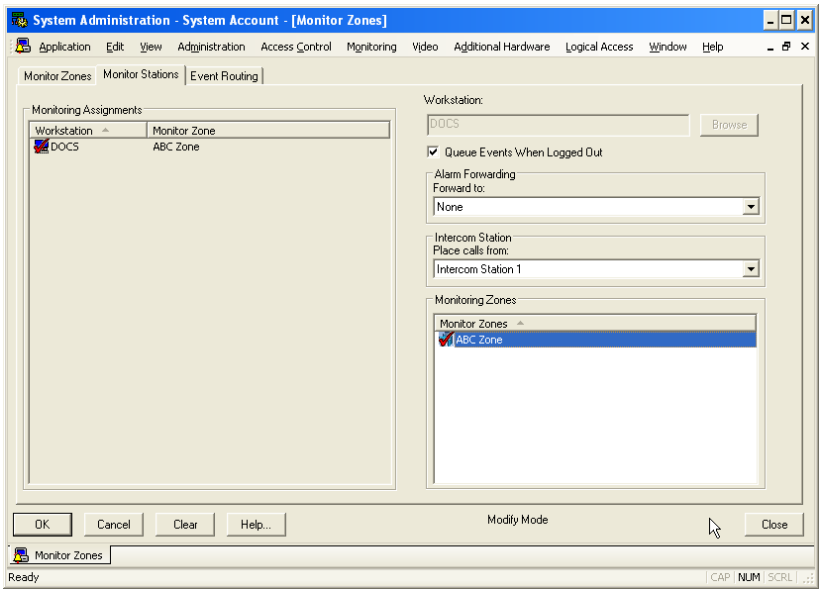
2. Click [Modify].
3. Make the changes you want.
   - To change the name, highlight the contents of the **Name** field, then type the new name.
   - If you want to assign a different map, simply select the name of the new map.
   - To add a device to this monitor zone:
     i. In the **Select** field, choose what device type to display in the Device window
     ii. Select one or more device(s) in the Device listing window.
     iii. If the device can have children devices, select whether to “Include All Child Devices” or “Specify Child Devices Individually”.
     iv. Optionally, select an event routing group in the Event Routing Groups list.
     v. Click [Assign].
   - To remove a device from this monitor zone:
     i. From the Device listing window located on the right side of the form, select the device entry that you want to remove.
     ii. Click [Remove]
     iii. Click [OK].

Delete a Monitor Zone

1. In the Monitor Zones list, select the name of the monitor zone you wish to delete.
2. Click [Delete].
3. Click [OK].

Monitor Stations Form

This form is used to, for a particular monitor zone, choose the workstations that will be able to monitor the zone. Note that assigning a workstation to a specific zone is optional. Such assignments can also be made “on the fly” upon login to the Alarm Monitoring software.



Monitoring Assignments

Lists workstations currently defined in the application, and their associated monitor zones.

Workstation

Selects the workstation that will be able to monitor the selected zone. The Workstation field is case insignificant and always stored in the database in uppercase letters. Letters are automatically converted to uppercase when you type a name into the field.

Browse

Enables you to search the network and choose the name of a workstation to insert into the Workstation field.

Queue Events When Logged Out

Selecting this check box configures the system to queue events while this monitoring station is logged off the system. When unselected, the system will still write events to the database while the monitoring station is logged off but the monitoring station operator must perform a historical trace to see these events.

Alarm Forwarding

Selects which monitor station, if any, will get forwarded alarms from the selected monitor zone.

Intercom Station

Selects which intercom station, if any, the workstation will use when using the Call Intercom feature.

Monitoring Zones

Selects the zone that will be monitored by the selected workstations. You can only select one monitoring zone for only one monitoring workstation at a time.

Add

Used to add a monitoring assignment.

Modify

Used to change a monitoring assignment.

Delete

Used to remove a monitoring assignment.

Mode

In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close

Closes the Monitor Zones folder.

Monitor Stations Form Procedures

Use the following procedures on this form.

Add a Monitoring Assignment

1. From the ***Monitoring*** menu, select ***Monitor Zones***. The Monitor Zones folder opens.
2. Select the Monitor Stations tab.
3. Click [Add].
4. Choose the workstation that will be able to monitor the selected zone. In the **Workstations** field, do one of the following:
   - Click [Browse] to display a Browse for Computer form. The form will contain a list of all workstations on your network. Click on the name of a workstation, then click [OK]. The name will be inserted into the **Workstation** field.
   - You can instead type the name of the workstation directly into the field. You must type the name absolutely correctly, or the application will not recognize it. For this reason it is better to use the [Browse] button to select a workstation.
5. From the Monitoring Zones listing window, select a monitor zone. Monitor zones are defined on the Monitor Zones form of this folder.
6. If you want this workstation to place calls using a specific intercom station when the user selects **Call Intercom** in Alarm Monitoring, select the intercom station. Intercom stations are defined in the ***Additional Hardware > Intercom Devices*** folder, and then select the Intercom Stations tab.
7. If you wish to have events for this monitoring station queued when no one is logged into this station, select the **Queue Events When Logged Out** check box.
8. Click [OK]. The workstation will be added in alphabetical order to the Monitoring Assignments list. You can assign more than one workstation on your network to the same monitor zone. However, each workstation can monitor only one zone.

Modify a Monitoring Assignment

1. From the Monitoring Assignments listing window, select the name of the assignment that you want to modify.
2. Click [Modify].
3. Make the changes you want to the fields.

Note: Note that you cannot modify the **Workstation** field for a monitoring workstation record once it has been added to the database. To rename a workstation, you must delete the current record and add a new one with all the same attributes (i.e. queue events and monitoring zone settings).

4. Click [OK] to save the changes, or click [Cancel] to revert to the previously saved values.

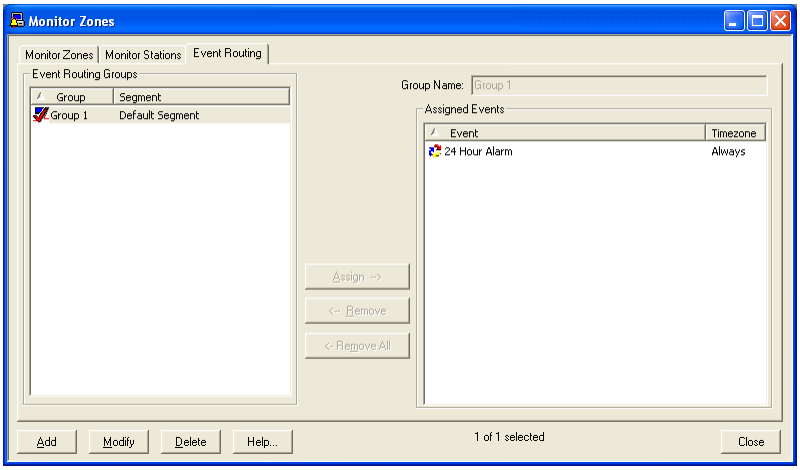
Delete a Monitoring Assignment

1. From the Monitoring Assignments listing window, select the name of the assignment that you want to delete.
2. Click [Delete].
3. Click [OK].

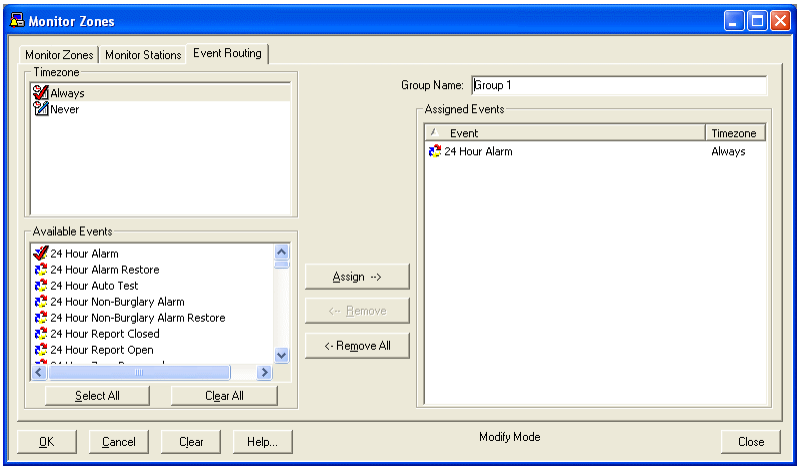
Event Routing Form

This form is used to define event routing groups, assign one or more events to a particular group, and assign (event + timezone) pairs to an event routing group. Event routing groups can be assigned to monitor zones using the Monitor Zones form. This enables system administrators to route specific types of alarm events to specific workstations during designated times on designated days.

Event Routing Form (View Mode)



Event Routing Form (Modify Mode)



Event Routing Groups

(view mode only) Lists current defined event routing groups by name. An icon precedes each entry.

Group Name

Indicates the name of the event routing group (a group of events).

Available Events

(modify mode only) List all currently defined events. An icon precedes each entry.

Timezones

Lists currently defined timezones. An icon precedes each entry.

Assigned Events

Lists (event + timezone) pairs that are included in the current event routing group. An icon precedes each entry.

Assign

Adds events selected in the Available Events list to the Assigned Events list. Each entry added will include the timezone name currently selected in the Timezones list.

Remove

Removes events selected in the Assigned Events list from that list.

Remove All

Removes all events included in the Assigned Events list from that list.

Select All

(modify mode only) Selects all entries in the Available Events list.

Clear All

(modify mode only) Deselects all selected entries in the Available Events list.

Add

Used to add an event routing group.

Modify

Used to change an event routing group.

Delete

Used to remove an event routing group.

Help

Displays online assistance for this form.

Mode

In view mode, indicates the record/selection count (such as “1 of 42”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close

Closes the Monitor Zones folder.

Event Routing Form Procedures

Use the following procedures on this form.

Add an Event Routing Group

1. Click [Add].
2. Type a name for the event routing group in the **Group Name** field.
3. In the Timezones list, highlight a timezone.

4. In the Available Events list, select one or more events that will be assigned to the selected timezone. To select an event, you must click on its icon. Or, use the arrow keys on your keyboard to highlight it, then press the spacebar. To deselect a selected event, click on it again (or highlight it and press the spacebar). Use the [Select All] and [Clear All] buttons to select or deselect all of the entries in the list.
5. Click [Assign]. Each of the selected events will be added to the Assigned Events list. Each entry will also include the selected timezone.
6. Repeat steps 3-5 for each combination of event(s) and a timezone that you wish to include in this event routing group.
7. Click [OK]. The event routing group name will then be listed in the Event Routing Groups window.

Remove Event and Timezone Pairs From an Event Routing Group

1. In the **Event Routing Groups** field, click on the name of the event routing group to select it. A selected entry has a checkmark on its icon.
2. Click [Modify].
3. In the Assigned Events list, select one or more event entries to be removed.
4. Click [Remove]. Each of the selected events will be removed from the Assigned Events list. If you select the [Remove All] button instead of the [Remove] button, all entries will be removed from the Assigned Events list.
5. Click [OK].

Delete an Event Routing Group

1. In the **Event Routing Groups** field, click on the name of the event routing group to select it. A selected entry has a checkmark on its icon.
2. Click [Delete].
3. Click [OK] to delete the group. Note that such an action may affect Event Routing Group assignments on the Monitor Zone form.

CHAPTER 45

Guard Tour Folder

The Guard Tour folder contains forms with which you can:

- Create, modify, and delete guard tours.
- Add checkpoints to tours.
- Assign minimum and maximum times to reach checkpoints.
- Associate actions with checkpoints.
- Associate messages with checkpoints.
- Associate tours with live video.
- Create tour instructions that can be viewed and printed prior to launching the tour from the Alarm Monitoring application.
- Create, modify, and delete tours groups.
- Schedule automatic guard tours.

The folder contains three forms: the Tours form, the Tour Groups form, and the Scheduler form.

The Guard Tour folder is displayed by selecting ***Guard Tour*** from the ***Monitoring*** menu, or by selecting the Guard Tour toolbar button.

Toolbar Shortcut

Guard Tour Overview

A guard tour provides a guard (a cardholder who has been specifically chosen to conduct a tour) with a defined set of tasks that must be performed within a specified period of time. Typical tasks include swiping a card at a checkpoint access reader or turning a key connected to an alarm panel input. *Checkpoints* are designated stops along a tour.

The guard tour management system records the location and timestamp for each checkpoint visited by a guard. The *checkpoint time* represents the time it should take to reach a particular checkpoint. All

checkpoints have minimum and maximum checkpoint times. A guard tour event is generated if a checkpoint is missed, reached early, on time, late, out of sequence, or is overdue.

A tour is considered complete when any of the following occur:

- All of the checkpoints on the tour have been reached, reached out of sequence, or missed.
- The tour is acknowledged as complete at a monitoring station.
- The tour is terminated at a monitoring station.

Guard tours are added in the Guard Tour folder in System Administration. For detailed information on how to configure a guard tour, refer to Add a Guard Tour on page 896. Once a tour has been configured, it can be launched and tracked from Alarm Monitoring.

Note: Guard Tour requires the configuration of a linkage server in the system.

Tours Form

This form is used to access the Tour Wizard, from where you can:

- Create, modify, and delete guard tours
- Add checkpoints to a tour
- Assign minimum and maximum times to reach checkpoints
- Associate actions with checkpoints
- Associate messages with checkpoints
- Associate the tour with live video
- Create tour instructions that can be viewed and printed prior to launching the tour from the Alarm Monitoring application

Listing window

Displays a list of currently defined guard tours and the checkpoints associated with each. A icon precedes each tour entry. A icon precedes each checkpoint entry.

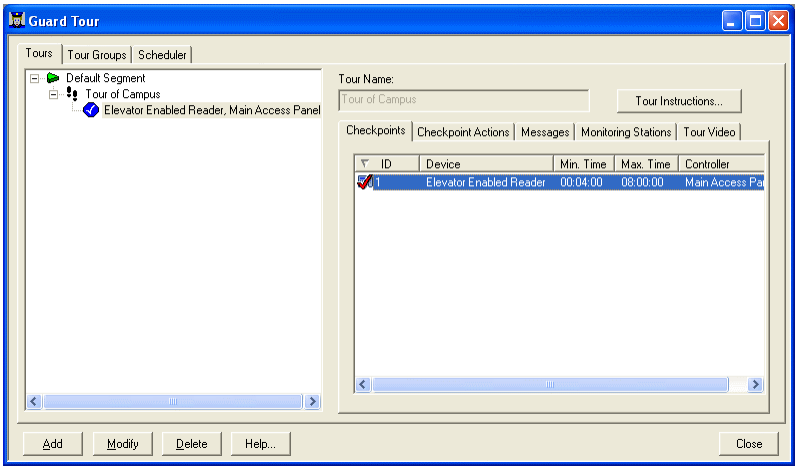
Tour Name

Displays the name of the selected tour.

Tour Instructions

When adding or modifying a tour, tour instructions can be added in the Tour Wizard. Click this button to view the instructions for this tour. Instructions can also be viewed prior to launching a tour from the Alarm Monitoring application.

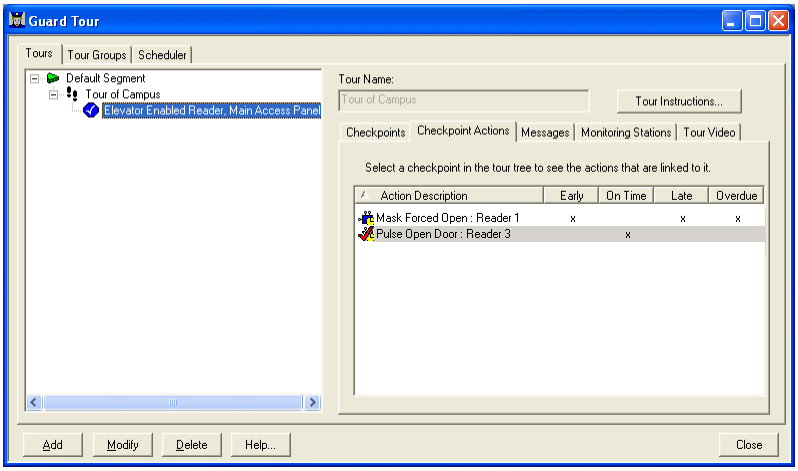
Tours Form (Checkpoints Sub-tab)



Checkpoints listing window

Displays a list of the checkpoints that have been assigned to the selected tour and configuration information pertaining to each. Checkpoints are assigned in the Tour Wizard.

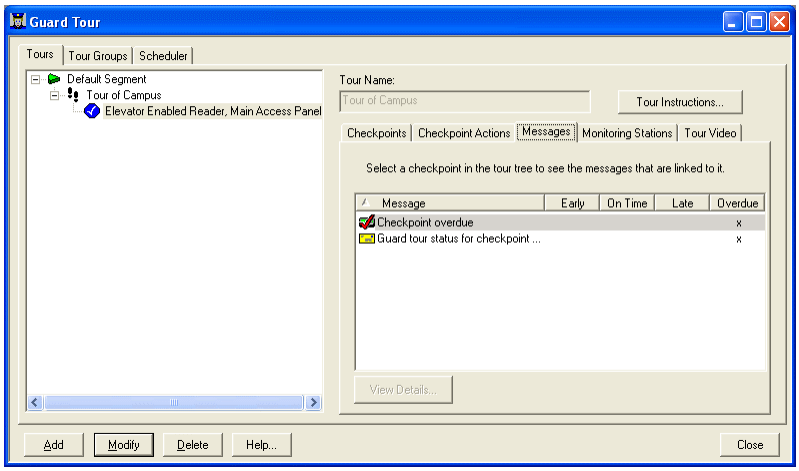
Tours Form (Checkpoint Actions Sub-tab)



Checkpoint actions listing window

Displays a list of the actions that have been linked to the checkpoint selected in the main listing window and configuration information pertaining to each. Checkpoint actions are linked in the Tour Wizard. A icon precedes each checkpoint action entry.

Tours Form (Messages Sub-tab)



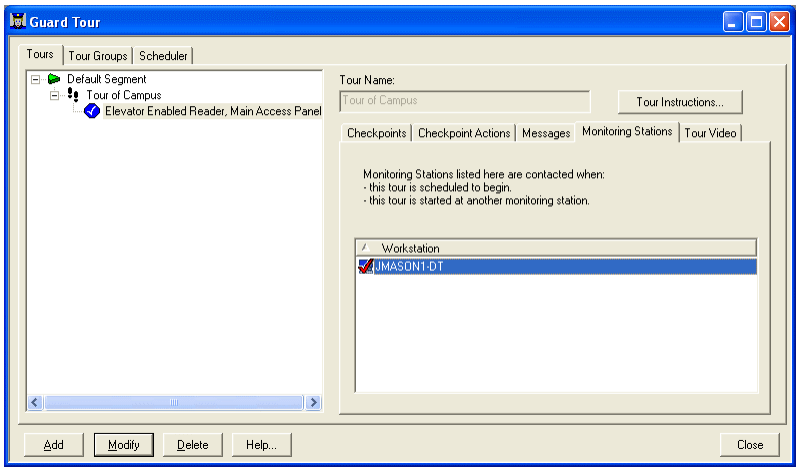
Messages listing window

Displays a list of the messages that have been linked to the checkpoint selected in the main listing window. Messages are linked in the Tour Wizard. A icon precedes each e-mail message entry. A icon precedes each pager message entry.

View Details

Click this button to display detailed information about the selected message.

Tours Form (Monitoring Stations Sub-tab)



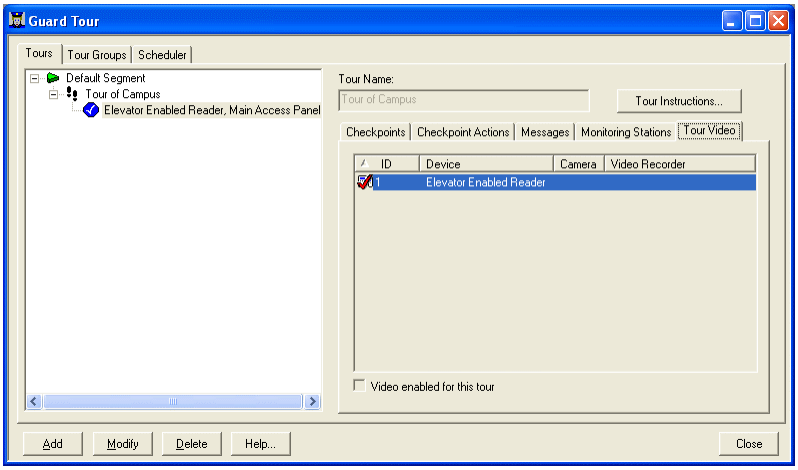
Monitoring stations listing window

Displays a list of the monitoring stations that have been assigned to the tour selected in the main listing window. Monitoring stations are assigned in the Tour Wizard. The monitoring stations in the list are contacted when:

- An automatic tour is scheduled to begin.
- The tour is started at another monitoring station.

A icon precedes each monitoring station entry.

Tours Form (Tour Video Sub-tab)



Tour video listing window

Displays a list of the checkpoints that have been assigned to the tour selected in the main listing window. If the checkpoint has been linked to a video device, the name of the device is also displayed.

Video devices are linked in the Tour Wizard. If the **Video enabled for this tour** check box was not selected in the Tour Wizard, this listing window is not enabled.

Video enabled for this tour

If this check box is selected, live video coverage of this tour will be displayed in the Alarm Monitoring application while the tour is taking place.

If the **Enable live video for this tour** check box was selected in the Tour Wizard during the configuration of tour video, then this check box will also be selected.

If the **Enable live video for this tour** check box was not selected in the Tour Wizard during the configuration of tour video, then this check box will not be selected.

Add

Click this button to start the Tour Wizard and add a tour.

Modify

Click this button to start the Tour Wizard and modify the tour that is selected in the main listing window.

Delete

Click this button to delete the tour that is selected in the main listing window.

Help

Click this button to display online assistance for this form.

Close

Click this button to close the Guard Tour folder.

Tours Form Procedures

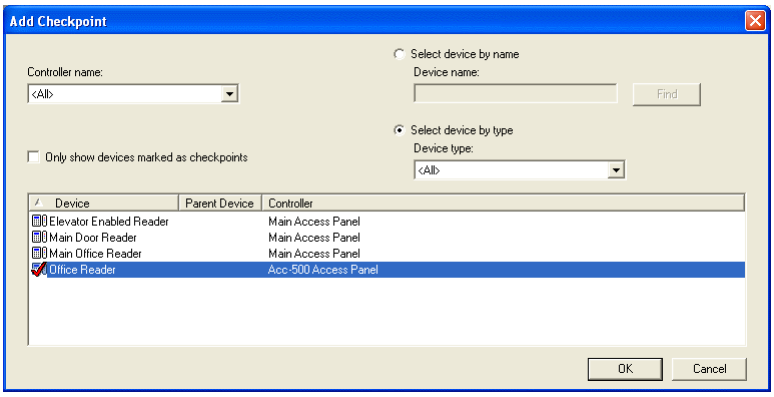
Use the following procedures on this form.

Add a Guard Tour

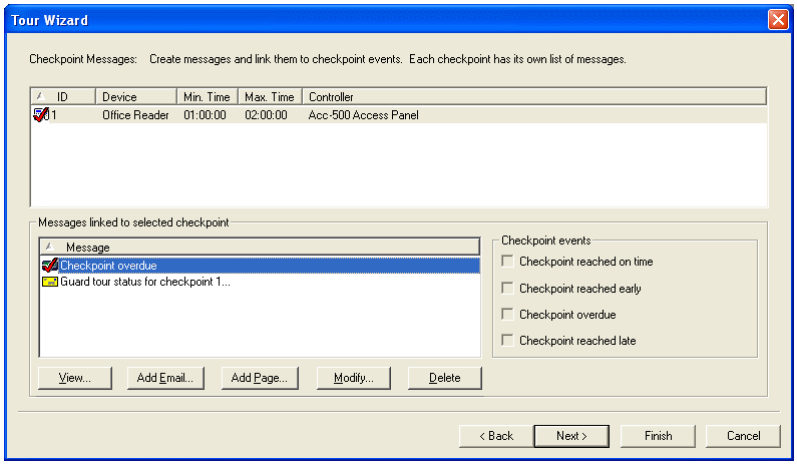
1. Select ***Guard Tour*** from the ***Monitoring*** menu. The Guard Tour folder displays.
2. Click [Add]. The Tour Wizard dialog displays.
3. In the **Tour name** field, enter a unique, descriptive name for the tour.
4. Click [Add]. The Add Checkpoint window opens.
5. From the **Controller name** drop-down list, select the name of the access panel that controls the checkpoint device that you want to add. If you select the **Only show devices marked as checkpoints** check box, only devices controlled by the selected access panel that have been marked as checkpoints will be displayed (devices can be marked as checkpoints when they are added or modified in the system). If this check box is not selected, all readers, reader inputs, and alarm inputs controlled by the selected access panel will be displayed.

Note: A device does not need to be marked as a checkpoint during its initial configuration in the system in order for it to be added as a checkpoint in a guard tour. The purpose of marking devices as checkpoints is for filtering the devices from which you can choose.

6. Do one of the following:
   - Select the **Select a device by name** radio button and type in the name of a device. Click [Find] to search the system for the name you typed. If you typed the entire name of a device, that device will be displayed in the listing window. If you typed the first letter(s) of a device name, all device names with matching first letter(s) will be displayed in the listing window. You must type at least one letter in the **Device name** field in order to search for a device by name.
   - Select the **Select a device by type** radio button to search for a device by type. Alarm inputs, readers, and reader inputs are the only types of devices that can be assigned as checkpoints.
7. Depending on your selections in steps 5 and 6, a list of devices will be displayed in the listing window. Click on a device to select it.



8. Click [OK]. The Tour Wizard proceeds. The name of the device you selected in step 7 is displayed in the Checkpoints listing window.



9. Repeat steps 4-8 for each device you want to add as a checkpoint.

Note: An ID number is automatically assigned to each device when it is added as a checkpoint. This number represents a checkpoint's sequence in a tour.

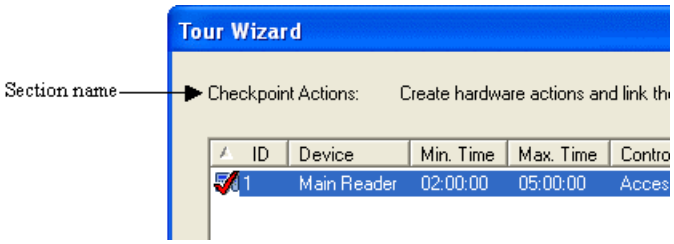
Example: a checkpoint with the ID number 1 is the first checkpoint that must be hit by a guard when the tour is run.

When there is more than one entry in the listing window, use [Move Up] and [Move Down] to rearrange the sequence order of the checkpoints.

10. In the Checkpoints listing window, click on a checkpoint to select it.
11. Enter the Checkpoint time, the time it should take for the tour guard to reach this checkpoint. Each checkpoint must have a minimum and a maximum checkpoint time.
    - Enter a Minimum minutes/seconds time. Example: 5 minutes, 30 seconds.
    - Enter a Maximum minutes/seconds time. Example: 10 minutes, 0 seconds.
12. Repeat steps 10 and 11 for each checkpoint.
13. You can click [Finish] and end the Tour Wizard. This guard tour is now available to be launched from a monitoring station running the Alarm Monitoring application. You can also click [Next] and assign checkpoint actions. If you click [Next], proceed to the "Assign Checkpoint Actions" procedure.

    To return to the Tour Wizard after you have clicked [Finish]:

    a. On the Tours form, select a tour entry from the main listing window.
    b. Click [Modify]. The Tour Wizard opens.
    c. Click [Next] until you reach the section of the Tour Wizard that you want to modify. The section name appears in the upper left hand corner of the wizard.



From this section	You can do this
Checkpoint Actions section	Assign Checkpoint Actions
Checkpoint Messages section	Create Messages and Link Them to Checkpoint Events
Monitoring Stations section	Assign Monitoring Stations to the Tour
Tour Video section	Link Camera Devices to Checkpoints
Tour Instructions section	Add Special Instructions

Assign Checkpoint Actions

Note: This procedure is optional.

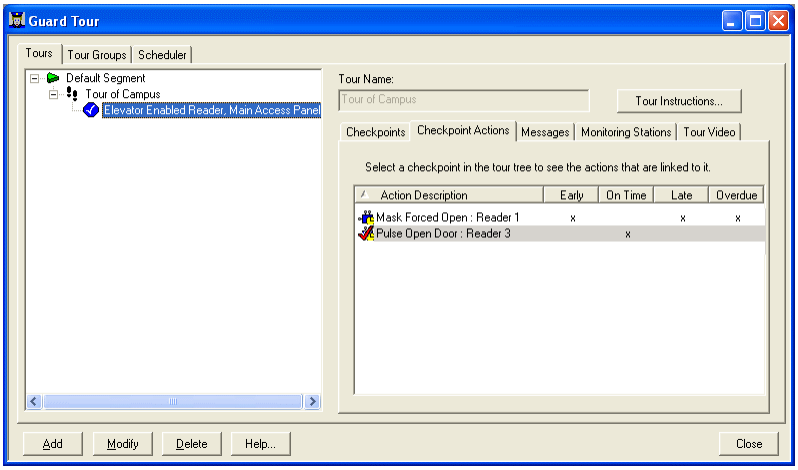
1. Skip this step if you are continuing from the procedure “Add a Guard Tour.” If you are not continuing:
   a. On the Tours form, select the guard tour entry you want to modify from the listing window.
   b. Select the Checkpoint Actions sub-tab.
   c. Click [Modify]. The Checkpoint Actions section of the Tour Wizard opens.
2. From the Checkpoint Actions section of the Tour Wizard, select a checkpoint from the listing window.
3. Click [Add]. The Add Action Wizard opens from where you can:
   - Assign specific hardware actions to checkpoints.

     Example: you can assign an action group that will turn on a light when a guard reaches the first checkpoint on a tour.
   - Assign specific groups of hardware actions to checkpoints.

     Example: you can assign an action that will turn on a light, open a door, and sound a buzzer when a guard reaches the second checkpoint on a tour.
4. Assign an action or an action group to the selected checkpoint. You must refer to the Actions appendix for detailed information on how to use the Add Action Wizard to assign an action. For more information, refer to Appendix A: Actions on page 1193.
5. Repeat steps 2-4 for each checkpoint action you want to assign.

Note: You can assign multiple actions to each checkpoint.

6. Select a checkpoint from the listing window. The action(s) you assigned to that checkpoint will be displayed in the Action Description listing window.
7. Select an action description from the listing window.



8. Select one or more of **Checkpoint events** check boxes.

   Example: if you assigned an open door action to a checkpoint, select which checkpoint events you want to trigger that action. If you want the door to open when the checkpoint is reached on time, select the **Checkpoint reached on time** check box. Multiple checkpoint events can trigger and action, and therefore, you can select more than one check box.
9. Repeat steps 6-8 for each checkpoint action.
10. You can click [Finish] and end the Tour Wizard. You can also click [Next] and create messages and link them to checkpoint events. If you click [Next], proceed to the "Create Messages and Link Them to Checkpoint Events" procedure.

Create Messages and Link Them to Checkpoint Events

Note: This procedure is optional.

1. Skip this step if you are continuing from the procedure "Assign Checkpoint Actions." If you are not continuing:
   a. On the Tours form, select the guard tour entry you want to modify from the listing window.
   b. Select the Messages sub-tab.
   c. Click [Modify]. The Checkpoint Messages section of the Tour Wizard opens.
2. From the Checkpoint Messages section of the Tour Wizard, select a checkpoint from the listing window.
3. To link the selected checkpoint to an e-mail message:
   a. Click [Add E-mail].
   b. The Add E-mail Message window opens. Click [To].
   c. The Select Recipient window opens, which contains a list of all currently defined e-mail recipients. Click on the name of a recipient to select it.

Note: E-mail recipients are added on the Recipients form of the Global Output Devices folder. If you need to add recipients, make sure to click [Finish] and not [Cancel] to exit the Tour Wizard.

   d. Click [OK].
   e. On the Add E-mail Message window, type in the Subject of your message.

f. In the **Message** field, type the actual content of the message. Notice that the number of characters contained in the message is displayed in the lower right corner of the window.

g. Click [OK].

h. Repeat steps a-g for each e-mail message you want to add.

4. To link the selected checkpoint to a pager message:

a. Click [Add Page].

b. The Add Pager Message window opens. Click [To].

c. The Select Recipient window opens, which contains a list of all currently defined pager recipients. Click on the name of a recipient to select it.

Note: Pager recipients are added on the Recipients form of the Global Output Devices folder. If you need to add recipients, make sure to click [Finish] and not [Cancel] to exit the Tour Wizard.

d. Click [OK].

e. On the Add Pager Message window, type the actual content of the message in the **Message** field. In the lower right corner of the window, the number of characters in the message will be updated as you type.

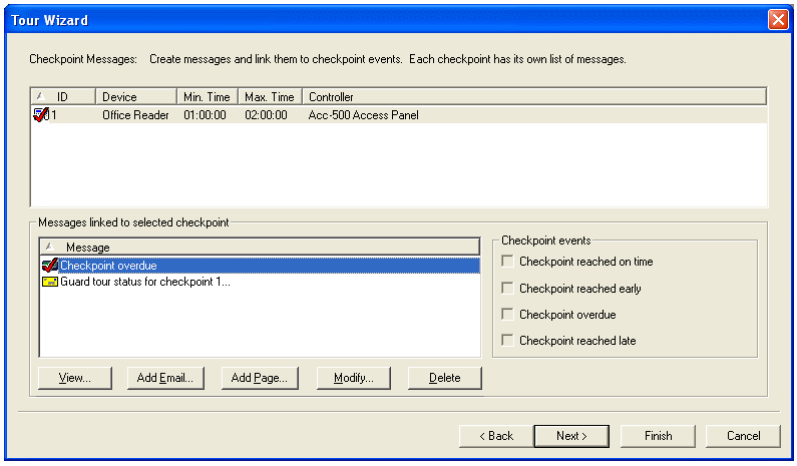
f. Click [OK].

g. Repeat steps a-f for each pager message you want to add.

Note: You can link multiple messages to each checkpoint.

5. Select a checkpoint from the listing window. The checkpoint messages you created will be displayed in the Message listing window.

6. Select a message from the listing window.



7. Select one or more of the **Checkpoint events** check boxes.

Example: if you linked an e-mail message to a checkpoint, select which checkpoint event you want to trigger that message to be sent. If you want the message to be sent when the checkpoint is reached on time, select the **Checkpoint reached on time** check box. Multiple checkpoint events can trigger a message to be sent, and therefore, you can select more than one check box.

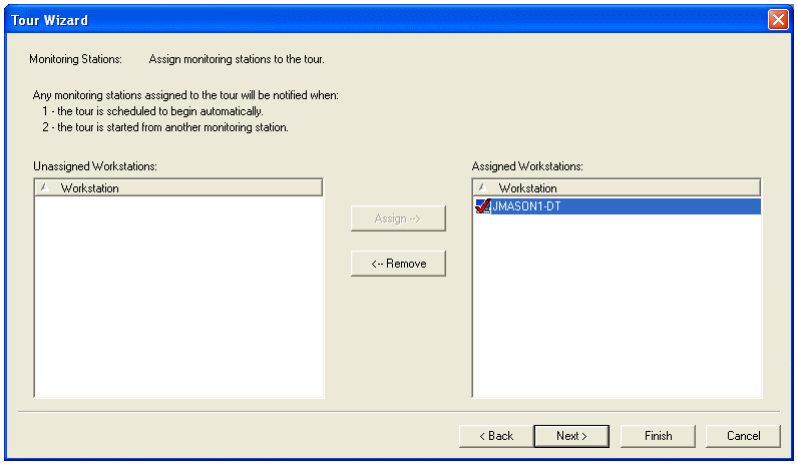
8. Repeat steps 6-8 for each checkpoint message.

9. You can click [Finish] and end the Tour Wizard. You can also click [Next] and assign monitoring stations to the tour. If you click [Next], proceed to the "Assign Monitoring Stations to the Tour" procedure.

Assign Monitoring Stations to the Tour

Note: This procedure is optional.

1. Skip this step if you are continuing from the procedure “Create Messages and Link Them to Checkpoint Events.” If you are not continuing:
   a. On the Tours form, select the guard tour entry you want to modify from the listing window.
   b. Select the Monitoring Stations sub-tab.
   c. Click [Modify]. The Monitoring Stations section of the Tour Wizard opens.
2. From the Monitoring Stations section of the Tour Wizard, select a workstation from the Unassigned Workstations listing window. Options include workstations that you added on the Monitor Stations form of the Monitor Zones folder and workstations that have run the Alarm Monitoring application at least once.
3. Click [Assign].



4. The workstation you assigned is displayed in the Assigned Workstations listing window. All workstations in the Assigned Workstations listing window will, in the Alarm Monitoring application, receive a “Guard Tour in Progress” status displayed next to the tour’s entry in the hardware tree when the tour is run. If this is an automatic guard tour, the assigned workstations will receive a notification message when the tour is scheduled to begin. For more information, refer to Scheduler Form on page 905. Repeat steps 2 and 3 for each workstation you want to assign to this tour.
5. You can click [Finish] and end the Tour Wizard. You can also click [Next] and link camera devices to checkpoints at this time. If you click [Next], proceed to the “Link Camera Devices to Checkpoints” procedure.

Link Camera Devices to Checkpoints

Note: This procedure is optional.

1. Skip this step if you are continuing from the procedure “Assign Monitoring Stations to the Tour.” If you are not continuing:
   a. On the Tours form, select the guard tour entry you want to modify from the listing window.
   b. Select the Tour Video sub-tab.
   c. Click [Modify]. The Tour Video section of the Tour Wizard opens.
2. From the Tour Video section of the Tour Wizard, select a checkpoint from the listing window.

3. Do one of the following:
   - Select the **Show all cameras** radio button to display every camera that is configured in the system in the Camera listing window.
   - Select the **Show all cameras that are linked to the checkpoint device** radio button to display only the cameras that are linked to the selected checkpoint's device to be displayed in the Camera listing window.

Note: Cameras are configured on the Camera form of the Digital Video folder. Cameras are linked to devices on the Device-Camera Links form of the Digital Video folder. To view the Digital Video folder, select ***Digital Video*** from the ***Video*** menu.

4. Select a camera from the listing window. This is the camera that will play live video when the tour is viewed in the Alarm Monitoring application.
5. Click [Assign].
6. Repeat steps 2-5 for each checkpoint you want to link to a camera.
7. Select the **Enable live video for this tour** check box if you want live video coverage of this tour to be displayed in the Alarm Monitoring application while the tour is taking place.

   If you want to save your configuration settings, but do not want to enable live video at this time, do not select this check box.
8. You can click [Finish] and end the Tour Wizard. You can also click [Next] and add special tour instructions at this time. If you click [Next], proceed to the "Add Special Instructions" procedure.

Add Special Instructions

Note: This procedure is optional.

1. Skip this step if you are continuing from the procedure "Link Camera Devices to Checkpoints." If you are not continuing:
   a. On the Tours form, select the guard tour entry you want to modify from the listing window.
   b. Click [Modify].
   c. In the Tour Wizard, click [Next] until you reach the Tour Instructions section.
2. In the Tour Instructions section of the Tour Wizard, type any special instructions for this tour (up to 2000 characters). These instructions can be viewed and printed from the monitoring station(s) assigned to this tour before the tour is launched.
3. Click [Finish].

Tour Groups Form

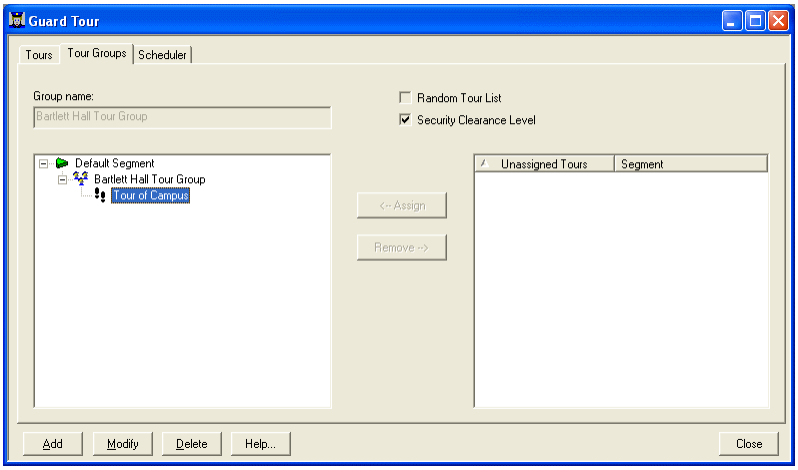
A tour group is a grouping of two or more guard tours. There are two reasons why you would want to create tour groups. They are:

Random Tour Lists. Random tour lists are used when scheduling automatic guard tours. An automatic guard tour is a tour that is scheduled to begin at a certain time. When an automatic guard tour is scheduled to begin, a notification message will be sent to the monitoring station(s) to which the tour is linked. When you schedule an automatic guard tour, you can choose to schedule either a particular tour, or a tour randomly selected from a tour group. When an automatic guard tour is scheduled for a tour group, the guard who is assigned to perform the tour will not know which tour to run until it is scheduled to begin. At that time, the system will randomly select one tour from the tour

group, and the guard will receive a notification message telling them which tour to run. For more information, refer to Scheduler Form on page 905.

Security Clearance Levels. Security clearance levels are a means of limiting the number of tour guards to choose from when a tour is launched. Particular security clearance levels will be assigned only to guards who will need access to areas where a tour will take them. When a tour is launched, only guards with the appropriate security clearance level for that tour will be listed.

Note: Tour guards are assigned security clearance levels on the Guard Tours form in the Cardholders folder.



Group name

Displays the name of the selected tour group.

Random Tour List

Select this check box if you want the tours in this tour group to be available for random selection when creating an automatic guard tour. For more information, refer to Scheduler Form on page 905.

Security Clearance Level

Select this check box if you want this tour group to represent a security clearance level. Security clearance levels are a means of limiting the number of tour guards to chose from when a tour is launched. Particular security clearance levels will be assigned only to guards who will need access to areas where a tour will take them. When a tour is launched, only guards with the appropriate security clearance level for that tour will be listed. Tour guards are assigned security clearance levels on the Guard Tours form in the Cardholders folder.

Tour group listing window

Displays a list of tour groups. A icon precedes each entry.

Assign

Click this button to assign an unassigned tour to a tour group. This button is enabled only when a tour is selected in the unassigned tours listing window. One tour can be assigned to multiple tour groups.

Remove
Click this button to remove a tour from a tour group. This button is enabled only when a tour is selected in the tour group listing window.

Unassigned tours listing window
Displays a list of all tours that are available to be assigned to a tour group. One tour can be assigned to multiple tour groups. A icon precedes each entry.

Add
Click this button to add a tour group.

Modify
Click this button to modify the selected tour group.

Delete
Click this button to delete the selected tour group.

Help
Click this button to display online assistance for this form.

Close
Click this button to close the Guard Tour folder.

Tour Groups Form Procedures

Use the following procedures on this form.

Add a Tour Group

1. Select ***Guard Tour*** from the ***Monitoring*** menu. The Guard Tour folder displays.
2. Click the Tours Group tab.
3. Click [Add].
4. In the **Group Name** field, enter a unique, descriptive name for the tour group. As you type, the name will appear in the tour group listing window preceded by a icon.
5. Select the **Random Tour List** check box if you want the tours in this tour group to be available for random selection when creating an automatic guard tour. For more information, refer to Scheduler Form on page 905.
6. Select the **Security Clearance Level** check box if you want this tour group to represent a security clearance level. Security clearance levels are a means of limiting the number of tour guards to choose from when a tour is launched. Particular security clearance levels will be assigned only to guards who will need access to areas where a tour will take them. When a tour is launched, only guards with the appropriate security clearance level for that tour will be listed. (Tour guards are assigned security clearance levels on the Guard Tours form in the Cardholders folder.)
7. In the unassigned tour groups listing window, select a tour.

Note: One tour can be assigned to multiple tour groups.

8. Click [Assign].

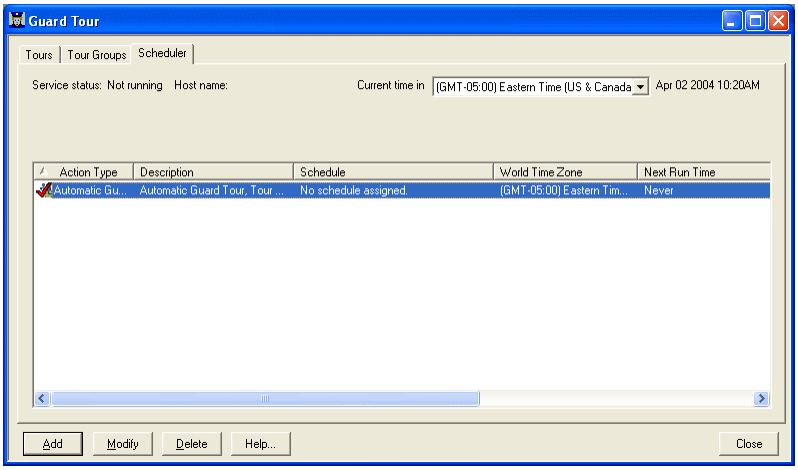
9. Repeat steps 7 and 8 for each tour you want to add to the tour group.
10. Click [OK].

Scheduler Form

The Scheduler form is used to automatically schedule guard tours. This form is available in the Guard Tours folder by selecting ***Guard Tour*** from the ***Monitoring*** menu. You can also display the Scheduler form (by itself) by selecting ***Scheduler*** from the ***Administration*** menu. Both forms perform the same function.

An *automatic guard tour* is a tour that is scheduled to begin at a certain time. When an automatic guard tour is scheduled to begin, a notification message is sent to alarm monitoring station(s) linked to the tour.

IMPORTANT: An automatic guard tour is automatically scheduled, not automatically started. When the notification message is received at alarm monitoring station(s), the tour must then be manually started.



Current time in

Select a world time zone to view the current time in a particular geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Listing window

Displays a list of currently defined automatic guard tour schedules.

Add

Click this button to open the Automatic Guard Tour Properties window and schedule an automatic guard tour.

Modify

Click this button to modify the selected automatic guard tour schedule.

Delete
Click this button to delete the selected automatic guard tour schedule.

Help
Click this button to display online assistance for this form.

Close
Click this button to close the Guard Tour folder.

Scheduler Form Procedures

Use the following procedures on this form.

Schedule an Automatic Guard Tour Action

1. Click the [Add] button on the Scheduler form of the Guard Tour folder. If your system is not segmented, proceed to step 3.
2. If your system is segmented, the Segment Membership window opens. Select a segment and click [OK].
3. The Automatic Guard Tour Properties window opens. Do one of the following:
   - Select the **Single Tour** radio button if you want to configure an automatic guard tour for a single tour. When selected, only single tours will be listed in the Tour/Tour Group listing window.
   - Select the **Randomly select tour from group** radio button if you want to configure an automatic guard tour that will be randomly selected from a tour group. When selected, only tours groups that are configured as random tour lists will be listed in the Tour/Tour Group listing window.
4. The monitoring stations that have been assigned to the selected tour or tour group will be displayed in the Monitoring Station listing window. Do one of the following:
   - If no monitoring stations have been assigned, or if you want to assign an additional monitoring station, click [Add]. The Select Monitoring Station window opens.
   - If you do not want to assign a monitoring station, proceed to step 8.
5. Click on a monitoring station to select it.
6. Click [OK]. The monitoring station you selected will be listed in the Monitoring Station listing window. All monitoring stations in the Monitoring Station listing window will receive a notification message, in the Alarm Monitoring application, when the tour is scheduled to begin.
7. Repeat steps 4-6 for each monitoring station you want to add.

Note: If you want to remove a monitoring station from the Monitoring Station listing window, click on an entry to select it, and then click [Remove].

8. Click the Schedule tab. Using the Schedule form, schedule this action. You must refer to the Scheduler folder chapter for detailed information on scheduling an action. For more information, refer to Chapter 24: Scheduler Folder on page 515.
9. Click [OK].

CHAPTER 46

Monitoring Options Folder

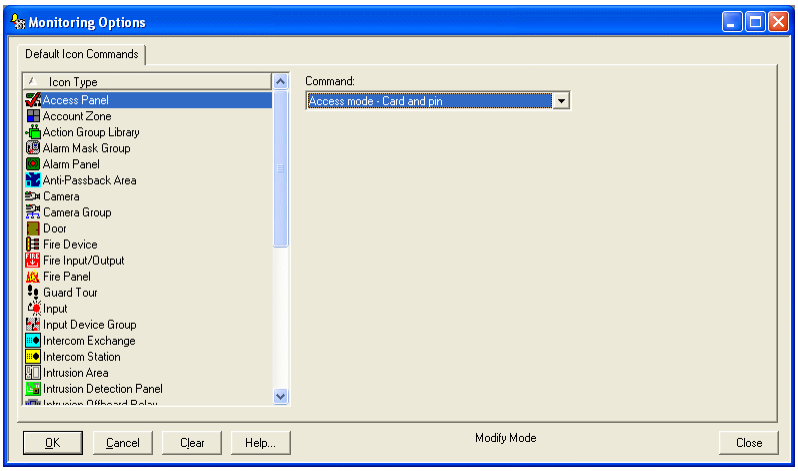
The Monitoring Options folder allows System Administrators to configure a command to be executed for an icon type on a system wide level. When an icon type, regardless of its state, is single or double-left clicked in Alarm Monitoring the command is executed. For example, an Alarm Monitoring operator can single or double-left click a door icon to unlock/lock a door.

Note: The type of click (single or double-left click) that executes the command for an icon is configured on a per user basis via Alarm Monitoring. For more information, refer to the Control Devices chapter in the Alarm Monitoring User Guide.

The Monitoring Options folder is displayed by selecting ***Monitoring Options*** from the ***Monitoring*** menu or by selecting the Monitoring Options toolbar button.

Toolbar Shortcut

Default Icon Commands Form



Icon Type listing window
(view mode only) Lists the available icon types that can be configured to execute a command.

Command
Lists the commands available for the selected icon type.

OK
Saves the changes and takes the Default Icon Commands form out of modify mode. The folder does not close when the [OK] is selected.

Modify
Allows you to add a command to the icon type or modify an existing one. The [Modify] button initially displays when the Monitoring Options folder opens. When this button is selected it automatically changes to [Cancel].

Cancel
Cancels the modifications without saving changes. The Monitoring Options folder does not close.

Clear
Removes the command assigned to the selected icon type and continues to keep the Default Icon Commands form in modify mode.

Help
Displays online assistance for this form.

Close
Closes the Monitoring Options folder. If you attempt to close the folder without saving changes, a message asks if you want to abandon your changes, giving you an option to save the changes.

Default Icon Commands Form Procedures

Use the following procedures on this form.

Configure Commands to Execute by Icon Type

1. Select ***Monitoring Options*** from the ***Monitoring*** menu or select the Monitoring Options toolbar button. The Default Icon Commands form opens.
2. Select an Icon Type from the list window.
3. Select the command you want executed from the **Command** drop-down list.
4. Repeat steps 2 and 3 for each icon type you want to configure. Multiple icon types can be configured with the same command.
5. Click [OK].

Note: After the icon types are configured to execute commands, Alarm Monitoring operators can execute these commands via the alarm window or map view. Be sure to either restart Alarm Monitoring or log out and log back in again. For more information about the single or double-left click commands, refer to the Control Devices chapter in the Alarm Monitoring User Guide.

Video

CHAPTER 47

Digital Video Folder

The Digital Video folder enables you to perform the following procedures:

- Configure video recorders and cameras
- Specify video device configurations
- Link cameras to devices
- Associate video actions with alarms
- Specify video recorder event-based configurations
- Add, modify, or delete an archive server
- Require user authentication for LNVR devices
- Configure standard video processing events (motion detection, blind camera detection, and brightness change) and camera-embedded IntelligentVideo events. For more information, refer to Video Processing Form on page 997.

The folder contains the following forms: the Video Recorder form, the Camera form, the Camera Inputs form, the Camera Outputs form, the Remote Monitor form, the Device-Camera Links form, the Alarm-Video Configuration form, the Video Event Text form, the Archive Server form, the Security form, the Video Processing form, and the PTZ Tour Server form.

You can display the Digital Video folder by selecting ***Digital Video*** from the ***Video*** menu, or by selecting the Digital Video toolbar button.

Toolbar Shortcut

Digital Video Recorder Overview

Lenel Digital Video Recorders include the LDVR-SP, LDVR-SP30, LDVR-408, LDVR-444, and LNVR recorders. Lenel Digital Video Recorders support the following features:

- Time-lapse recording mode
  - Records video at a low frame rate when little or no activity is detected

- Event Locking
  - Locks video so that it cannot be deleted during recording
- Real time preview of live video and playback of recorded video from multiple channels
- PTZ control
- Real time recording of all active channels
- Motion detection with selectable sensitivity and area
- Blind camera detection
- Real time export of any video channel (in native format)
- Archiving
- Security
  - Unauthorized access is prevented by Windows security
  - For more information, refer to Security Form on page 992.

Virtual Matrix Switcher for LDVR and Third Party Recorders

LDVR and third party recorders integrated via the SDK can now be set up using a virtual matrix switcher if no physical matrix switcher is present. For more information, refer to Add a Matrix Switcher (Real and Virtual) on page 1038.

Things to note about the virtual matrix switcher:

- Multi-drop (connecting multiple cameras to the same COM port) is supported if the connecting cameras also support it. When using multi-drop, enter the drop-in address instead of the camera channel.
- When adding cameras to the virtual matrix switcher the address of the camera is used for the channel (the address is configured through the camera's DIP switches.)

For more information refer to the Digital Video Hardware User Guide.

LDVR-SP

The LDVR-SP recorders are a family of board based recorders that record video from analog cameras. The LDVR-SP supports up to 4 boards per unit (per recorder) and up to 32 channels per recorder.

LDVR-SP Recorder Features

- Real time, multi-stream MPEG1 video recording
- 30 fps multiplexed over each board (up to 8 channels)
- PTZ control with matrix switcher
  - Serial connection between matrix switcher and Communication Server.
  - Analog video connection (coaxial cable with BNC connectors) between matrix switcher and LDVR-SP and, between matrix switcher and PTZ camera.
  - In OnGuard, create a matrix switcher. Link each camera configuration, to a channel number on the matrix switcher (on the Camera form > Communication sub-tab).
- PTZ control with virtual matrix switcher
  - Serial connection between Pelco Spectra Dome III camera and Communication Server, which may or may not be on the LDVR-SP.
  - Analog video connection (coaxial cable with BNC connectors) between Pelco Spectra Dome III camera and LDVR-SP.

- Multi-drop support with virtual matrix switcher
  - RS-485 and RS-422 standards support multi-drop. Pelco Spectra Dome III cameras with RS-485 or RS-422 connections can be connected to the same COM port on the Communication Server.
  - In OnGuard, create a virtual matrix switcher. For each camera configuration, enter the drop-in address instead of the channel number (on the Camera form > Communication sub-tab). This address needs to match the address set on the camera via a dip switch.
  - RS-232 standards do not support multi-drop; only one camera is supported. The drop-in address for an RS-232 camera connection must be “1”.
- Audio recording
- Dry contacts
- Video export to standard MPEG1 format

LDVR-SP Video Channel Features

- Adjustable MPEG1 compression and frame rate
  - Any one channel can have a maximum of 15 fps
  - Each channel can have a unique frame rate as long as the total fps for all the channels does not exceed 30 fps
- Motion detection and blind camera detection configured on the Camera form > Communication tab.
- Flexible assignment of audio channels

LDVR-SP30

The LDVR-SP30 supports up to 4 boards per unit (recorder), and up to 16 channels per recorder.

LDVR-SP30 Recorder Features

- Real time, multi-stream MPEG1 video recording
- PTZ control with matrix switcher
  - Serial connection between matrix switcher and Communication Server.
  - Analog video connection (coaxial cable with BNC connectors) between matrix switcher and LDVR-SP30 and, between matrix switcher and PTZ camera.
  - In OnGuard, create a matrix switcher. Link each camera configuration, to a channel number on the matrix switcher (on the Camera form > Communication sub-tab).
- PTZ control with virtual matrix switcher
  - Serial connection between Pelco Spectra Dome III camera and Communication Server, which may or may not be on the LDVR-SP30.
  - Analog video connection (coaxial cable with BNC connectors) between Pelco Spectra Dome III camera and LDVR-SP30.
- Multi-drop support with virtual matrix switcher
  - RS-485 and RS-422 standards support multi-drop. Pelco Spectra Dome III cameras with RS-485 or RS-422 connections can be connected to the same COM port on the Communication Server.
  - In OnGuard, create a virtual matrix switcher. For each camera configuration, enter the drop-in address instead of the channel number (on the Camera form > Communication sub-tab). This address needs to match the address set on the camera via a dip switch.

  - RS-232 standards do not support multi-drop; only one camera is supported. The drop-in address for an RS-232 camera connection must be “1”.
- Audio recording
- Dry contacts
- Video export in standard MPEG1 format

LDVR-SP30 Video Channel Features

- Adjustment of MPEG1compression and frame rate
  - Any one channel can have a maximum of 30 fps (25 fps for PAL)
- Motion detection and blind camera detection configured on the Camera form > Communication tab.
- Flexible assignment of audio channels
- Real time viewing of live video or, recorded playback of video for up to 4 active channels
- Archiving is limited to 4 channels if recorded at 30 fps

LDVR- 408

The LDVR-408 supports 2 boards per unit (recorder), and up to 16 channels per recorder.

LDVR- 408 Recorder Features

- Real time, multi-stream MPEG4 video recording
- Video resolution that applies to every camera associated with the recorder
  - High resolution 2CIF (640 x 240) or low resolution CIF (320 x 240)
  - High resolution: 45 fps (40 for PAL) multiplexed across an 8-channel board
  - Low resolution: 60 fps (50 for PAL) multiplexed across an 8-channel board
- PTZ control with matrix switcher
  - Serial connection between matrix switcher and Communication Server.
  - Analog video connection (coaxial cable with BNC connectors) between matrix switcher and LDVR-408 and, between matrix switcher and PTZ camera.
  - In OnGuard, create a matrix switcher. Link each camera configuration, to a channel number on the matrix switcher (on the Camera form > Communication sub-tab).
- PTZ control with virtual matrix switcher
  - Serial connection between Pelco Spectra Dome III camera and Communication Server, which may or may not be on the LDVR-408.
  - Analog video connection (coaxial cable with BNC connectors) between Pelco Spectra Dome III camera and LDVR-408.
- Multi-drop support with virtual matrix switcher
  - RS-485 and RS-422 standards support multi-drop. Pelco Spectra Dome III cameras with RS-485 or RS-422 connections can be connected to the same COM port on the Communication Server.
  - In OnGuard, create a virtual matrix switcher. For each camera configuration, enter the drop-in address instead of the channel number (on the Camera form > Communication sub-tab). This address needs to match the address set on the camera via a dip switch.
  - RS-232 standards do not support multi-drop; only one camera is supported. The drop-in address for an RS-232 camera connection must be “1”.
- Audio recording

- Dry contacts

LDVR- 408 Video Channel Features

- Adjustment of MPEG4 compression and frame rate
  - Any one channel can have a maximum of 7.5 fps while recording at low resolutions
  - Any one channel can have a maximum of 3.75 fps while recording at high resolutions
- Motion detection configured on the Camera form > Communication tab.
- Real time recording of up 16 active channels
- Flexible assignment of audio channels

LDVR- 444

The LDVR-444 supports up to 4 boards per unit (recorder), and up to 16 channels per recorder.

LDVR- 444 Recorder Features

- Real time, multi-stream MPEG4 video recording
- Video resolution that applies to every camera associated with the recorder
  - D1 (720 x 480)
  - 4CIF (640 x 480)
  - CIF (320 x 240)
- PTZ control with matrix switcher
  - Serial connection between matrix switcher and Communication Server.
  - Analog video connection (coaxial cable with BNC connectors) between matrix switcher and LDVR-444 and, between matrix switcher and PTZ camera.
  - In OnGuard, create a matrix switcher. Link each camera configuration, to a channel number on the matrix switcher (on the Camera form > Communication sub-tab).
- PTZ control with virtual matrix switcher
  - Serial connection between Pelco Spectra Dome III camera and Communication Server, which may or may not be on the LDVR-444.
  - Analog video connection (coaxial cable with BNC connectors) between Pelco Spectra Dome III camera and LDVR-444.
- Multi-drop support with virtual matrix switcher
  - RS-485 and RS-422 standards support multi-drop. Pelco Spectra Dome III cameras with RS-485 or RS-422 connections can be connected to the same COM port on the Communication Server.
  - In OnGuard, create a virtual matrix switcher. For each camera configuration, enter the drop-in address instead of the channel number (on the Camera form > Communication sub-tab). This address needs to match the address set on the camera via a dip switch.
  - RS-232 standards do not support multi-drop; only one camera is supported. The drop-in address for an RS-232 camera connection must be “1”.
- Audio recording
- Dry contacts
- Video export in standard MPEG4 format

LDVR- 444 Video Channel Features

- Adjustment of MPEG4 compression and frame rate
  - Any one channel can have a maximum of 30 fps (25 fps for PAL)
- Motion detection and blind camera detection configured on the Camera form > Communication tab.
- Flexible assignment of audio channels
- Real time viewing of live video or recorded playback of video for up to 4 active channels
- Archiving is limited to 4 channels if recorded at 30 fps

LNVR

The LNVR provides network recording for up to 63 IP cameras.

A list of supported cameras and features for each LNVR version can be found in the Video Tools section of the Customer Self-service Center on the Lenel website: http://customer.lenel.com/

There are no boards inside the recorder.

LNVR Recorder Features

- Real time, multi-stream MJPEG and MPEG4 video recording
- Security: unauthorized access is prevented by OnGuard
- Video export to standard ASF and proprietary format (.LNR) files

LNVR Video Channel Features

- Multiple video resolutions based on camera capabilities
- Adjustable image quality and frame rate
  - Maximum frame rate of 30 fps per channel
- Event based video recording
  - Triggered by any IntelligentVideo alarm or by any event configured on the Alarm -Video Configuration form
- IntelligentVideo image processing
- Motion detection and blind camera detection configured on the Video Processing form
- Supports surveillance-only mode
- PTZ support for the following configurations:
  - Pan-Tilt-Zoom (PTZ) IP cameras
  - Pan-Tilt (PT) IP cameras
  - Zoom (Z) cameras
  - IP cameras with ability to control PTZ housing
  - Video Servers with ability to control PTZ housing
  - For more information, refer to the Digital Video Hardware User Guide.
- Failover recorder creates a virtual channel for a camera
- Signal loss detection on Axis video servers
  - Note that for Axis 2400 and 2400+ servers, up to 4 analog cameras can be configured. Therefore, video signal loss and restored events should be tied to a specific channel (on the Alarm Definitions form).

goVision R1 and R1.5

The goVision R1 and R1.5 recorders support viewing up to 4 channels of recorded video and a maximum of 24 live connections.

goVision R1 and R1.5 Recorder Features

- Real-time embedded operating system
  - Full PTZ control
  - Multi-screen views
  - Customizable GUI
- Powerful video processing
  - 4/8/16 channel configurations at full frame rate, full resolution
  - Embedded MCU
  - High performance DSP hardware compression
  - Real-time H.264 video compression
- Supports advanced hard disk functionality
  - Sleep mode
  - S.M.A.R.T. functionality
  - FAT32 file system
- Advanced network functionality
  - Available web client for viewing and configuration
  - TCP, UTP, RTP, DHCP
  - Instant firmware upgrades
  - Remote manageability, free client application and web application

goVision R1 and R1.5 Video Channel Features

- Live video transmitted from the recorder to client software is transmitted at CIF resolution, 6 fps, 320 KB/sec.
- Multiple record modes
  - Event recording
  - Motion detection
  - Always on
  - Manual record configuration
- OnGuard IntelligentVideo image processing (forensic use)
- Up to 16 camera inputs
- Alarm inputs and outputs
- Full PTZ control
- Video signal loss detection

goVision R2

The goVision R2 recorder supports viewing up to 48 channels of live or recorded video.

goVision R2 Recorder Features

- Embedded Linux operating system

  - Full PTZ control
  - Multi-screen views
  - Customizable GUI
- Powerful video processing
  - 4/8/16 channel configurations at full frame rate, full resolution
  - Embedded MCU
  - High performance DSP hardware compression
  - Real-time H.264 video compression
- Supports advanced hard disk functionality
  - Sleep mode
  - S.M.A.R.T. functionality
  - FAT32 file system
  - Grouping and redundant recording
- Advanced network functionality
  - Available web client for viewing and configuration
  - TCP, UTP, RTP, DHCP
  - Instant firmware upgrades
  - Remote manageability, free client application and web application
- Lenel embedded IntelligentVideo (IV) events (On recorders equipped with optional IV DSP daughter card)
  - Supports the following subset of IV Events: SmartVMD, Invalid Camera, Loitering, Object Crosses a Region, Object Detection, and Object Left Behind
  - Recorder-generated IV events are displayed in Alarm Monitoring as generic events with the appropriate event text
- Supports IP cameras

goVision R2 Video Channel Features

- Live video transmitted from the recorder to client software is transmitted at the default settings of CIF resolution, 6 fps, variable bitrate, 320 Kbits/sec
- Multiple record modes
  - Event recording
  - Motion detection
  - Always on
  - Manual record configuration
- OnGuard IntelligentVideo image processing (real-time and forensic use)
- Up to 16 analog camera inputs plus up to 4 IP cameras
- Alarm inputs and outputs
- Full PTZ control
- Video signal loss detection
- Privacy masks

NetDVMS

By default, the NetDVMS is configured to accept 10 client connections at once. A “connection” is any application or service that is communicating with the NetDVMS recorder. The Communication

server will use 25 connections; if the Linkage server is configured it will use one connection. Each external client, Alarm Monitoring, and VideoViewer application running on a client machine is also another connection.

To increase the maximum number of client connections, use the Image Server Administrator on the NetDVMS. The number of connections possible is also dependent upon available system resources. The recommended number for the maximum client connections is 75.

Notes: If the Communication Server is offline, missed events from the NetDVMS will not be received when the Communication Server comes back online.

When the NetDVMS Administrator application is closed on the DVR, all NetDVMS services are restarted which will result in Communication Lost and Restored alarms in Alarm Monitoring.

If a camera is enabled or disabled on a slave recorder there may be a delay of up to 60 seconds before the status is updated in Alarm Monitoring.

Requirements

To get information about device status and receive events from the NetDVMS recorder, NetCentral must be configured in NetDVMS Administrator. For information on configuring NetCentral, please refer to the NetDVMS documentation. The following requirements must be met during configuration:

- The OnGuard software can only store one set of credentials per video recorder. The login credentials must be the same for the NetDVMS login, for allowing a NetCentral connection, and for the NetDVMS in the OnGuard software. All slave recorders must have the same login credentials as the master recorder.
- The port configured on each NetDVMS recorder for allowing a NetCentral connection must be the default port (1237). This port must also be opened in the firewall on each NetDVMS recorder.
- The NetDVMS must be configured to accept connections on port 8080. This setting is configured on the NetDVMS recorder with the Image Server Administrator application.
- To view video in Remote Monitor or the VideoViewer Browser-based Client, the NetDVMS username must be set to “sp911” and the password must be set to “lenel”.

NetDVMS Recorder Features

- Support for MJPEG, MPEG-4 and H.264 video formats (Configurable on the NetDVMS)
- On-event or manual (peer-to-peer) push-live-video to external client (recipients are imported with NetDVMS configuration and video is sent manually from Alarm Monitoring or configured to send on alarm in System Administration)
- Supports IP cameras (Configurable on the NetDVMS)

NetDVMS Video Channel Features

- PTZ control
  - Continuous PTZ
  - 50 presets per PTZ camera (Configured on the NetDVMS and controllable from OnGuard)
- Motion detection (Configured on the NetDVMS with the option to receive alarms configured in System Administration)

Video Recorder Failover and Redundancy

OnGuard supports failover recorders (secondary recorders) for IP cameras. Failover recorders record and process video only when the primary recorder is offline.

When the primary recorder goes offline, an alarm is generated and the failover recorder begins recording video. Users can view live video from the time the alarm was generated on the failover recorder. The failover recorder uses the same workstation and IntelligentVideo algorithms and channel parameters as the primary recorder. When the primary recorder comes back online, a restored alarm is generated, the primary recorder connects to the IP camera and resumes recording. When both the recorders are online, users can view uninterrupted recorded video.

The redundancy feature is a full-time failover solution. In a failover configuration, video channels are recorded to the primary recorder unless it goes offline, at which time recording occurs on the secondary recorder. In a redundant configuration, video channels are recorded to both the primary and secondary recorders regardless of the status of the primary recorder.

Redundant channel events are not sent to Alarm Monitoring. For example, if a motion detection event occurs on a camera with redundancy configured, the alarm will only be sent to Alarm Monitoring from the primary recorder.

Failover and redundancy can be configured on the Camera > Connection sub-tab for individual IP cameras or on the Video Recorder > Failover sub-tab for all cameras configured for the LNVR.

Time-Lapse Recording

Time-lapse mode slows the rate at which video is recorded. Motion detection can be used to trigger recording at the normal (non-time-lapse) rate when activity occurs.The primary motivation of this feature is to save storage space on the video recorder.

LDVR cameras have a built in motion detection mechanism which is used in conjunction with time-lapse to trigger the normal recording rate. This motion detection feature is always on, but may need additional configuration to filter out excess motion. For more information, refer to Configure Time-Lapse Recording for LDVR Cameras on page 968.

Time-lapse recording mode can be triggered into event recording mode by a wide variety of events with LNVR cameras. LNVR cameras do not have an automatic motion detection mechanism, and require additional configuration to trigger event mode recording. Many different combinations of device-camera links and alarm-video configurations can be used. Some examples of events that can be configured to trigger event recording include: door forced open alarms, input alarms, and video events. For more information, refer to Configure Time-Lapse Recording with Motion Detection for LNVR Cameras on page 968.

Integration with Storage Calculator

Camera information can be exchanged between System Administration and the Storage Calculator application. This enables a more accurate prediction of system resource usage and the easy addition of new cameras to the system.

The System Administration export includes the data on the Capacity sub-tab of the Camera form to provide statistics for your network to the Storage Calculator for estimating the bandwidth and storage needs for new cameras. To export the camera configuration for an LNVR, right-click the video recorder and select Export. This file can then be imported into the Storage Calculator application.

System Administration can also import cameras using the IP Camera Wizard to add cameras that have had their initial configuration calculated in the Storage Calculator. For more information, refer to Import IP Cameras from the Storage Calculator on page 937.

Note: Statistics may differ for the same camera between System Administration and the Storage Calculator. The camera information available in System Administration is based on the actual usage on your system and can vary depending on network traffic, activity level in the scene, etc.

For more information about import and export within the Storage Calculator, refer to the help available from within the Storage Calculator application.

Video Recorder Form

The following form elements are found commonly with both LDVR and LNVR recorders.

Listing window
Lists currently defined video recorders, the workstation they are connected to, and the segment that each recorder belongs to (if segmentation enabled).

Name
A descriptive name for the video recorder. This should be a “friendly” name assigned to video recorder making it easy to identify. Each name must be unique and contain no more than 32 characters.

Online
If selected, the video recorder will be online and the Communication Server will attempt to communicate with it.

Video Recorder Type
Specifies the type of video recorder.

Recorder Web Page
Opens the selected recorder’s configuration Web page where you can modify settings for the recorder. This button displays when you configure goVision recorders and OpenAccess Alliance Program (OAAP) recorders that support this feature.

Detect
Connects to the video recorder to determine the video recorder type.

Update Capabilities
Connects to the video recorder and obtains a list of camera capabilities for the firmware version currently installed.

Add
Create a new video recorder entry.

Modify
Enables changes to be made to the selected video recorder entry.

Delete
Removes the selected video recorder entry.

Help
Displays online help for this topic.

Close

Closes the Digital Video folder.

Video Recorder Form Right-Click Menu

When the Video Recorder form is not in add or modify mode, you can right-click any recorder to display the following menu options:

Choose this option	To do this
Add	Create a new video recorder entry.
Modify	Enable changes to be made to the selected video recorder entry.
Delete	Delete the selected video recorder entry.
Copy	Copy the selected video recorder entry.
Select Item	Select a video recorder entry.
Clear Item	Deselect the selected video recorder entry.
Select All	Select all video recorder entries.
Clear All	Deselect all selected video recorder entries.
Download	Download settings to the selected video recorder.
Set Clock	Used to set the time on the video recorder. **Note:** This option is only supported for goVision recorders and OAAP video recorders that support this feature.
Export To File	Export the LNVR cameras to an XML file for import into the Storage Calculator application.
Import From File	Use the IP Camera Wizard to import cameras from a file to the LNVR.
Import From Recorder	Used to import cameras that were configured on the video recorder. This option can also be used to update OnGuard with any changes to the camera configuration that have been made on the video recorder. This option is only available for NetDVMS, goVision, and OAAP video recorders that support this feature.
Camera Wizard	Add multiple LDVR cameras using the Camera Wizard.

Import Cameras Dialog

The Import Cameras dialog is used to import the camera configuration from video recorders. The Import Cameras dialog is opened using the ***Import From Recorder*** right-click menu item. This option is only available for NetDVMS, goVision, and OAAP video recorders that support this feature.

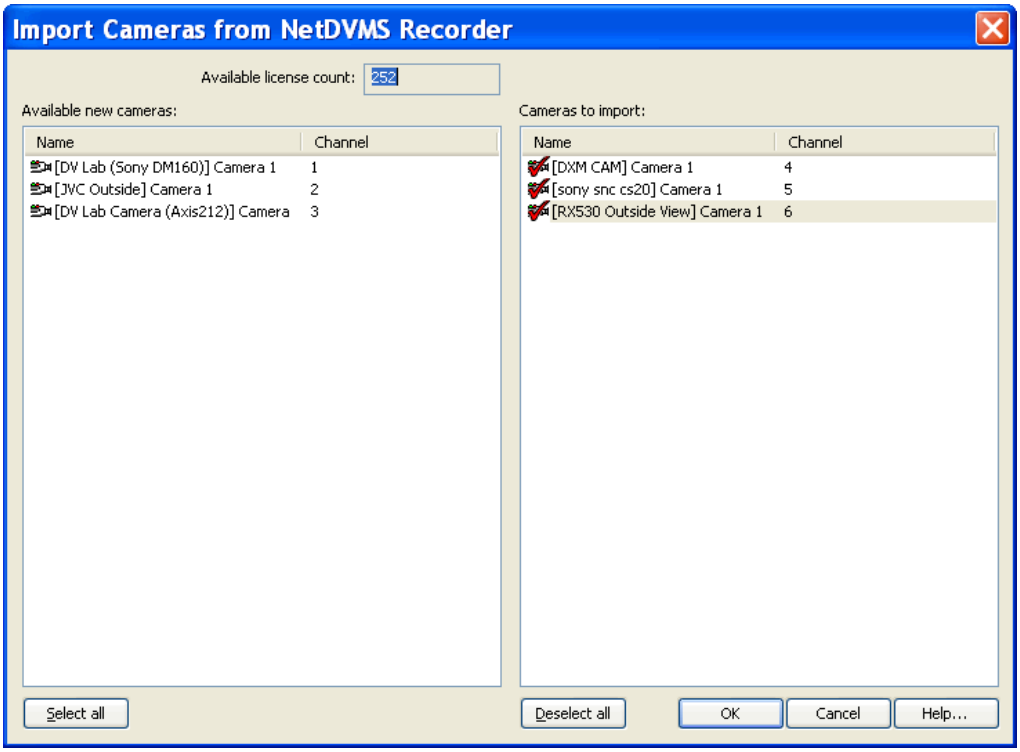
The Communication Server service must be running when you import video channels from a NetDVMS, goVision, or OAAP recorder.

When you import video channels from a NetDVMS master recorder, all of the video channels from the slave recorder will also be imported as channels for the master. If you import channels from the slave recorder also, you will have duplicate video channels.

When you import video channels that have PTZ presets configured on the NetDVMS, the presets will also be imported. These PTZ presets will be available from the Video Player as read-only presets with the same name configured in the NetDVMS.

Note: When you import from a NetDVMS recorder, alarms may be lost if they come in during the short window while which the import is being performed.

The Import Cameras dialog allows you to select which cameras will be imported from the video recorder. The dialog also displays the number of available camera channels remaining on the license.



Import Cameras from a NetDVMS, goVision, or OAAP Video Recorder

To import cameras from a NetDVMS, goVision, or OAAP video recorder that supports this feature:

1. Start System Administration and select the ***Video*** **>** ***Digital Video*** menu item.
2. The Video Recorder form is displayed. Right-click the video recorder you want to import from and select **Import from Recorder**.
3. The Import Cameras dialog is displayed:
   a. Select (place a check mark beside) the cameras you want to import from the Available new cameras listing window. Alternatively you can click the [Select all] button to select all of the cameras in the listing window.
   b. If you want to change the name of a camera, click the camera name in the listing window to enter edit mode, then enter the new name.

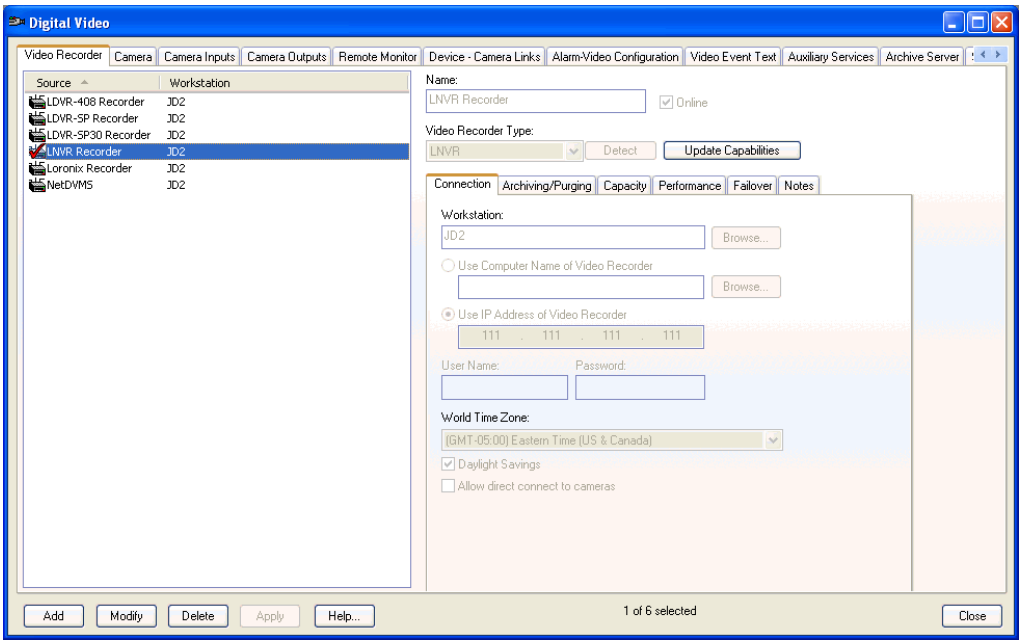
Note: Camera names must be unique. If the camera name specifies matches another camera name in the database you will not be able to import cameras until you specify a different name.

c. Click [OK] to import the cameras.

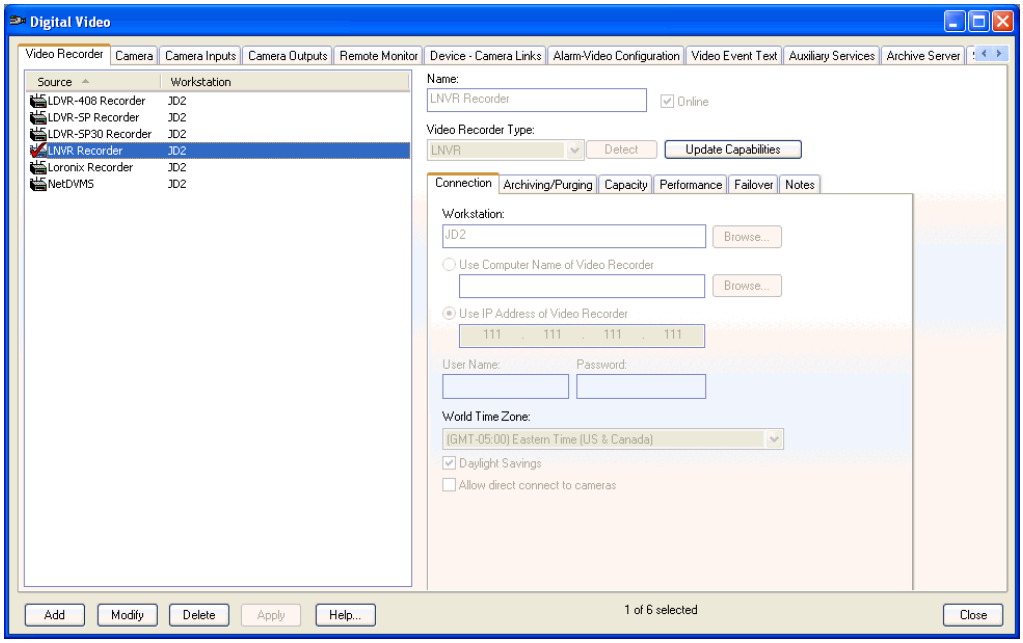
IMPORTANT: The NetDVMS configuration must be imported whenever cameras are added or deleted from a NetDVMS recorder. To do this, first open the Administrator application on the master NetDVMS and close it without making changes. Then, use the Import Cameras dialog to import the camera configuration from the NetDVMS.

Video Recorder Form (Connection Sub-tab)

The following Connection sub-tab displays for Generic Video, LDVR-SP, LDVR-SP30, LDVR-408, LDVR-444, NetDVMS, and Loronix recorders.



The following Connection sub-tab displays for LNVR, goVision, and OAAP recorders. Available fields may vary depending on which features the recorder supports.



LNVR Security and Passwords

When you install LNVR firmware, you have an opportunity to set the LNVR access level. There are two access level options; “LNVUsers” or “Everyone”. The “LNVUsers” is a local user group created during LNVR installation. You can add members to the “LNVUsers” group during the installation or afterwards by clicking Start, then ***Programs > Lenel Network Recorder*** and running the LNVR Setup. For more information, refer to “Install the LNVR Firmware” in the Digital Video Hardware User Guide.

In addition to setting access levels, you have an option to set a specific Windows account to be used by OnGuard to connect to the LNVR. To do this, enter the account’s user credentials (user name and password) on the Connection sub-tab of the Video Recorder form. Alternatively, you can make OnGuard use the current interactive user Windows account by leaving the username and password fields blank.

Note: These credentials will be ignored when OnGuard applications or services are running on the same machine as LNVR. Instead the account used by the OnGuard application or service running will be used for authentication. The following accounts have access to LNVR: Members of the LNVUsers group, local system account, and accounts which have LNVR services configured to run.

There are two benefits of using the “LNVUsers” group and a specific Windows account combination:

- The specific Windows account is the only one that needs to be added to “LNVUsers” group as compared to adding an interactive user Windows account for every OnGuard user.
- Data transferred between LNVR and OnGuard is encrypted.

Video Recorder Form - Connection Sub-tab Fields

Workstation

The workstation the video recorder connects to. The Communication Server should run on the workstation you select. This workstation will be referred to as the “OnGuard server.” The

workstation name must be the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse
Opens a Browse for Computer window, from which you can select a workstation.

Use IP Address of Video Recorder
Select this radio button if you want to use the IP address of the video recorder.

Use Computer Name of Video Recorder
Select this button if you want to use the computer name of the video recorder.

Browse
Opens a Browse for Computer window, from which you can select the name of a computer.

User Name and Password
The user name and password for the specific Windows account used by OnGuard to connect with the specified video recorder. If you leave these fields blank, OnGuard will use the interactive user Windows account. For more information, refer to LNVR Security and Passwords on page 925.

World Time Zone
The world time zone for the selected video recorder's geographical location. The selections in the drop-down are listed sequentially and each include:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of the countries or cities located in that world time zone.

Daylight Savings
Select this check box if you want to properly convert between various time formats for daylight savings.

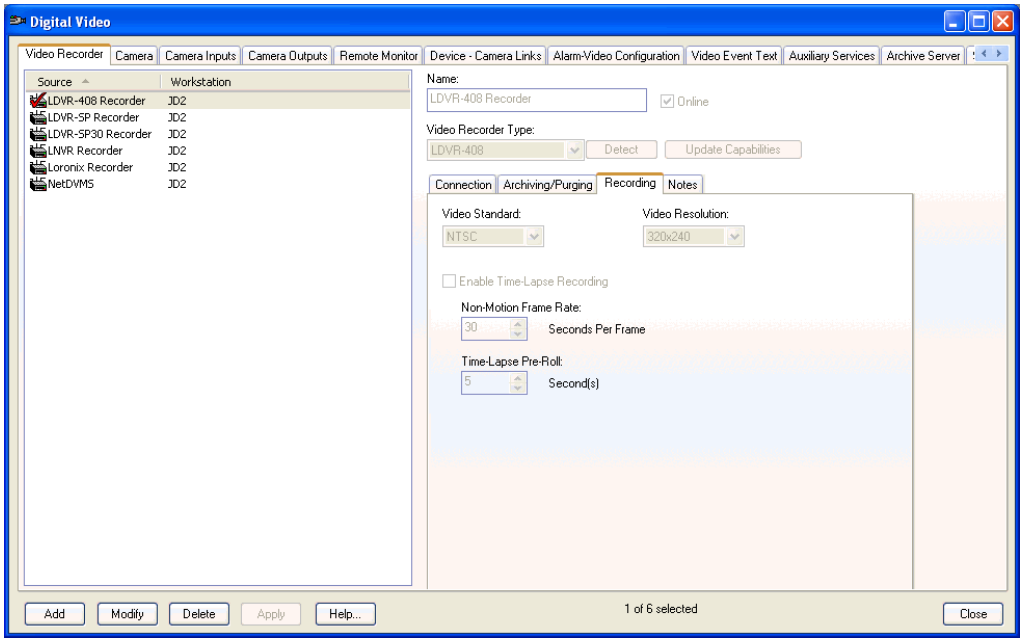
Allow direct connect to cameras
Enables a direct connection to IP cameras for live video display if the LNVR is offline.

Automatic clock synchronization
Sets the time on the goVision or OAAP recorder to the time on the Communication Server.

Video Recorder Form (Recording Sub-tab)

Note: The Recording sub-tab does not display for the LNVR, Generic Video, or Loronix recorder.

The following Recording sub-tab displays for LDVR-SP, LDVR-SP30, LDVR-408, LDVR-444 recorders. Note that the **Video Resolution** drop-down does not display for the LDVR-SP or LDVR-SP30 recorder.



Video Standard

Select a video standard.

Video Resolution

The resolution every camera associated with the specified video recorder. This field only applies to LDVR-408 and LDVR-444 recorders.

Enable Time-Lapse Recording

Select this check box if you want the frame rate for the selected video recorder to be lower when no motion is detected. The lower frame rate is called the *Non-Motion Frame Rate*. Time-lapse recording must also be enabled for the camera, on the Record Settings sub-tab of the Camera form. Motion Detection is always on for cameras configured with LDVR-SP, LDVR-SP30, LDVR-408,or LDVR-444 video recorders. Whenever motion is detected, the camera will switch to continuous recording mode.

Non-Motion Frame Rate

The frame rate video is recorded at, when no motion is detected. This option is used only when time-lapse recording is enabled for the particular camera.

Time-Lapse Pre-Roll

The number of seconds you want to cache video prior to the instant motion is detected. This option is used only when time-lapse recording is enabled for the particular camera. Pre-roll video is recorded at the full frame rate.

Video Recorder Form (Archiving/Purging Sub-tab)

Note: The Archiving/Purging sub-tab does not display for generic video or Loronix recorders.

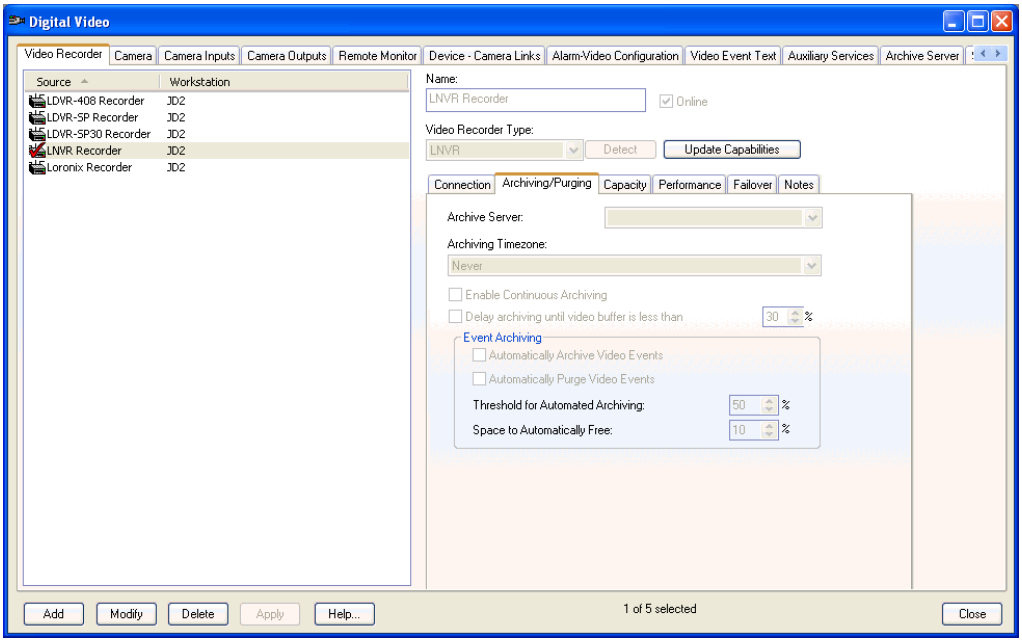
Video events are created when a video alarm occurs or when a device with a camera link generates an alarm. These alarms can be configured to lock the video associated with them so that the video is not overwritten on the recorder.

Recording video creates numerous large files. To keep enough drive space free for new video files, you must either purge the locked video files or archive the files. *Purging* means that after a specified period of time (or specified amount of disk space remains), the old video files are deleted. If you are purging the files, the Archive Server service can be run on any computer on the network. When purging, it is common to run the Archive Server service on the same computer that the Communication Server is run on.

Archiving means that the most recent files are kept on the video recorder (generally just a few days), while older files are stored on tape. OnGuard uses Remote Storage Solution, an application that comes with Windows Server 2003, to migrate the video files from disk to tape.

Note: This is not a backup solution, it is a storage solution. You must make a copy of the tape to have a backup!

The following Archiving/Purging sub-tab displays for LDVR-SP, LDVR-SP30, LDVR-408, LDVR-444, and LNVR recorders.



Archive Server

Lists all archive servers in the database that are appropriate for the recorder's segment. Archive server options are created on the Archive Server form in the Digital Video folder. For more information, refer to Add an Archive Server on page 991. The selected archive server archives and purges video from the recorder. If this field is blank, archiving does not occur for the video recorder.

Archiving Timezone

A specific time to archive video. For example, many people avoid archiving during business hours and instead archive during the night. This field lists all timezones in the database. Choices include:

– **Always** - This is the standard way archiving is done. If selected, the archive server archives video from the recorder as soon as the recorder has one block of video.

- The duration of the video block is configurable on the archive server, and is one hour by default.
- **Never** - If selected, archiving from the recorder does not occur.
- **User-defined timezones** - If a specific timezone is selected, the archive server archives new video during the selected timezone. It continues archiving until all the video from the recorder is archived. Archiving resumes when it is in that timezone again (provided the recorder has enough video to archive).

Timezones are added on the Timezones form, which opens when you select the ***Access Control*** > ***Timezones*** menu option and click the Timezones tab.

Enable Continuous Archiving

Select this check box if you want video continually archived, 24 hours a day. The cameras must also be configured for continuous archiving.

Delay archiving until video buffer is less than____%

If selected, the archive server delays archiving until the video buffer (the amount of video on the recorder) is less than the specified amount. The recommended buffer size is 30%. The buffer decreases when the oldest video on the recorder is overwritten and increases when the archive server archives video blocks and therefore moves the archiving point forward.

This option is commonly used when the storage on the archive server is not much larger than the storage on the video recorders. Without this option enabled, most of the video would be duplicated on the video recorders and the archive server. With this option enabled, only parts of the oldest video on the recorder are duplicated.

Automatically Archive Video Events

Select this check box if you want video events to be automatically archived off the video recorder. Event archiving is supported for LDVR-408, LDVR-444, LDVR-SP, LDVR-SP30, and LNVR recorders.

Automatically Purge Video Events

Select this check box if you want video events to be automatically purged from the video recorder.

Threshold for Automated Archiving

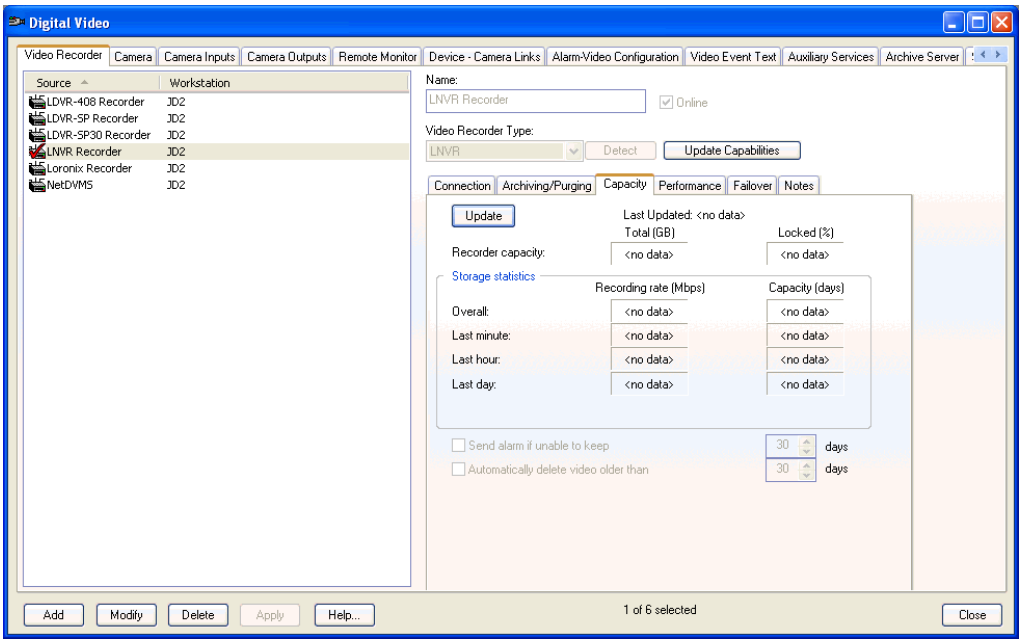
The percent of video recorder disk space to use for video events, before automatic archiving or purging begins.

Space to Automatically Free

The percent of video recorder disk space that should be freed up before archiving or purging stops.

Video Recorder Form (Capacity Sub-tab)

The following Capacity sub-tab displays for LNVR recorders.



Update

Connects to the video recorder to retrieve the current storage statistics.

Recorder capacity

Displays the amount of storage available on the recorder. This value does not include the amount of space left free as configured in the LNVR Storage configuration.

Overall

Displays the total average recording bit rate in Mbps. According to this rate, the recorder should be able to store the number of days worth of video listed in the Capacity (days) column.

Last minute

Displays the average recording bit rate in Mbps for the last minute. According to this rate, the recorder should be able to store the number of days worth of video listed in the Capacity (days) column.

Last hour

Displays the average recording bit rate in Mbps for the last hour. According to this rate, the recorder should be able to store the number of days worth of video listed in the Capacity (days) column.

Last day

Displays the average recording bit rate in Mbps for the last day. According to this rate, the recorder should be able to store the number of days worth of video listed in the Capacity (days) column.

Send alarm if unable to keep

Select the check box to generate an alarm if the capacity (days) falls below a specific value.

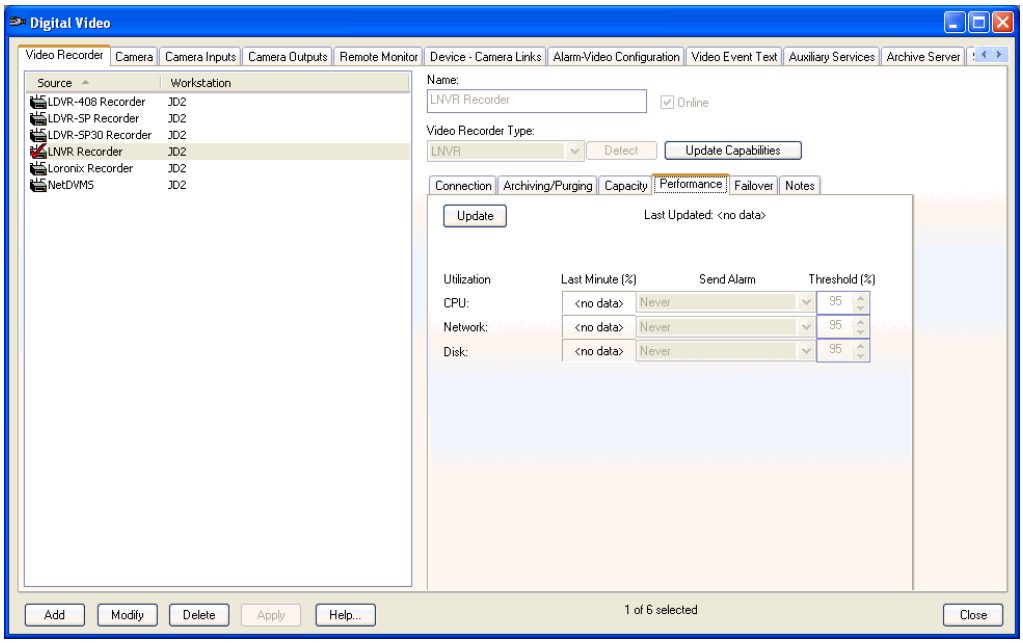
Automatically delete video older than

Select this check box to limit the number of days that video is stored on the recorder. Locked and unlocked video older than the specified number of days will be automatically deleted twice each

day. The value can be in the range of 1 to 3650 days. Locked video that has not been archived will be deleted after the specified number of days. Activation of this feature will not delete archived video located on the archive server.

Video Recorder Form (Performance Sub-tab)

The following Performance sub-tab displays for LNVR recorders.



Update

Connects to the video recorder to retrieve the current storage statistics.

CPU

Displays the percent utilization of the CPU for the last minute. To generate an alarm if the percentage reaches a certain level, select the timezone in the Send Alarm column, and set the level in the Threshold (%) column.

Network

Displays the percent utilization of the network for the last minute. To generate an alarm if the percentage reaches a certain level, select the timezone in the Send Alarm column, and set the level in the Threshold (%) column.

Disk Read

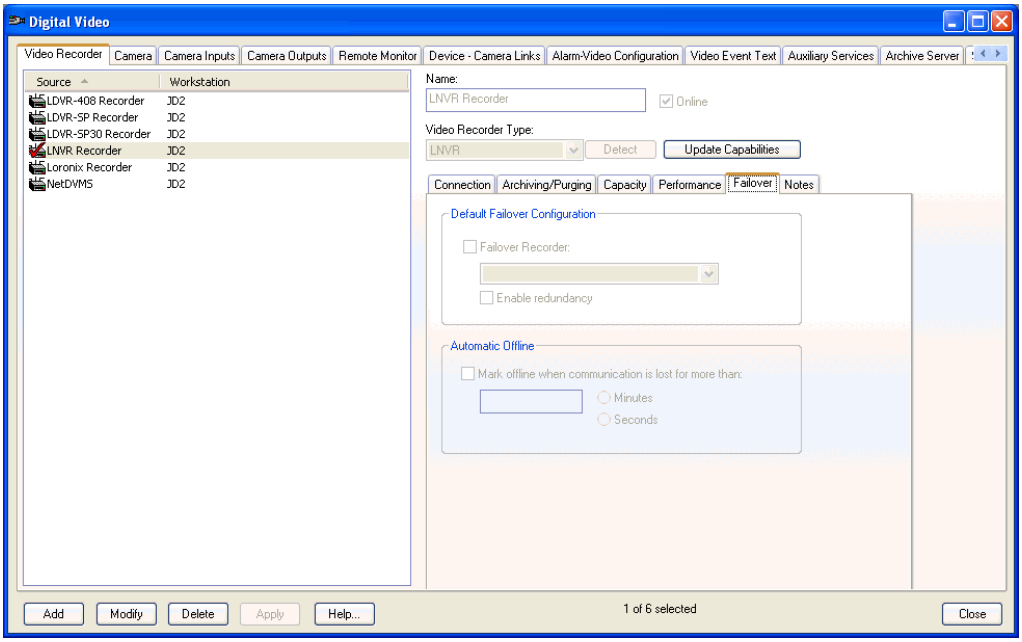
Displays the percent utilization of the disk read for the last minute. To generate an alarm if the percentage reaches a certain level, select the timezone in the Send Alarm column, and set the level in the Threshold (%) column.

Disk Write

Displays the percent utilization of the disk write for the last minute. To generate an alarm if the percentage reaches a certain level, select the timezone in the Send Alarm column, and set the level in the Threshold (%) column.

Video Recorder Form (Failover Sub-tab)

The following Failover sub-tab displays for LNVR recorders.



For more information, refer to Video Recorder Failover and Redundancy on page 920.

Failover Recorder

Select this check box to enable a failover recorder for all of the IP cameras configured on this video recorder, then select the secondary recorder from the drop-down.

Enable Redundancy

Select this check box to enable continuous failover mode.

Automatic Offline

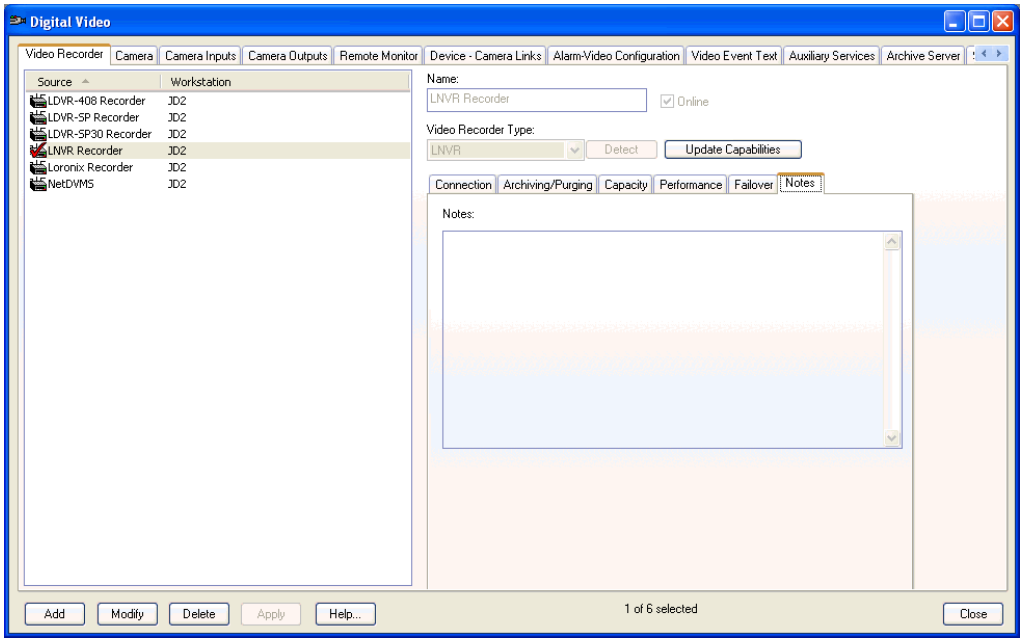
This feature enables you to limit the amount of time that the system will attempt to reconnect to the video recorder after it has gone offline. After the specified time has elapsed, an alarm will be generated in Alarm Monitoring to indicate that the recorder has been marked offline and the system will no longer attempt to reconnect to the recorder.

To reset Automatic Offline after it has been activated, the video recorder must first be marked online in Alarm Monitoring. The system will then continually attempt to reconnect to the recorder disregarding the Automatic Offline settings even if it remains physically offline. Once the system has successfully reconnected to the recorder, Automatic Offline will be reset and will once again be activated if the recorder goes offline.

Mark offline when communication is lost for more than

Select this check box to enable the Automatic Offline feature. Specify an amount of time in the text box and select the appropriate radio button for **Minutes** or **Seconds**. Setting low values for timeout on systems with small or problem networks may cause the video recorder to be marked offline frequently.

Video Recorder Form (Notes Sub-tab)



Notes

Enter information about the device. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

Video Recorder Form Procedures

Refer to the Video Recorder sub-tab tables if you have questions on fields or how to populate them.

Add LNVR Video Recorders

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this video recorder is assigned to.
   b. Click [OK].
4. In the **Name** field, enter a unique, descriptive name for the video recorder.
5. Select “LNVR” from the drop-down.
6. On the Connection sub-tab:
   a. Enter the workstation the video recorder connects to. If configuring LNVR for failover, you must be connected to the same Communication Server as the primary LNVR.
   b. Do one of the following:
      - Select the **Use IP Address of Video Recorder** radio button and enter an IP address.

- Select the **Use Computer Name of Video Recorder** radio button and enter the computer's name.

c. Enter the user name and password if desired. For more information, refer to LNVR Security and Passwords on page 925.

d. Click [Detect] to connect to the LNVR and verify the recorder type.

e. Select the world time zone for the selected video recorder's geographical location.

f. Select the **Daylight Savings** check box if you want to properly convert between various time formats for daylight savings.

g. If desired, select the **Automatically delete video older than** check box and enter the number of days after which locked and unlocked video should be deleted.

7. On the Archiving/Purging sub-tab:

a. Select an archive server and a timezone to archive. If you do not want to archive video from the video server, leave the **Archive Server** field blank and continue to step 8.

b. Select the **Enable Continuous Archiving** check box if you want video to be continually archived, 24 hours a day. Each camera must also be configured to archive continuously.

c. Select the **Delay archiving until video buffer is less than __%** check box if you want the archive server to delay archiving until the video buffer is less than the specified amount. The recommended buffer size is 30%.

d. Select the **Automatically Archive Video Events** check box if you want video events to be automatically archived or the **Automatically Purge Video Events** check box if you want video events to be automatically purged from the video recorder.

e. In the **Threshold for Automated Archiving** spin box, choose the percentage of video recorder disk space to be used by video events before automatic archiving begins.

f. Select In the **Space to Automatically Free** spin box, choose the percentage of disk space that should be freed up before the archiving or purging should stop.

8. Click [OK].

9. The Monitor Zone Assignments dialog is displayed. Select the monitor zone(s) you wish to assign the video recorder to and click [OK].

10. Click [Update Capabilities] to obtain an update of camera capabilities from the LNVR for the currently installed firmware. This information is stored in the database and enables you to configure cameras even if the LNVR is offline.

Note: Before you use this video recorder, download your settings. To do this, right-click the video recorder in the video recorder listing window and select "Download". Downloading is highly recommended even if the recorder appears to be in working order because it prevents the loss of configuration parameters.

Add LNVR Failover Video Recorders

Notes: Alarm Monitoring users should log out and log back in to the application when changes are made to the configuration of a failover recorder.

It is recommended to have the same version of firmware on the primary and failover recorders.

Failover recorders can be configured on a per-recorder or per-channel basis. Each channel on the primary recorder may be assigned a different failover recorder. To add an LNVR failover video recorder, complete the Add LNVR Video Recorders on page 933. Be sure to mark the failover recorder online and connect it to the same Communication Server the primary LNVR connects to.

To configure failover for all of the cameras configured on the LNVR, select the **Failover Recorder** check box on the Video Recorder > Failover sub-tab and select the secondary recorder from the drop-down.

To configure failover for an individual camera channel, or to configure different failover recorders for multiple cameras configured on the same LNVR, select the secondary recorder from the **Failover Recorder** drop-down on the Camera > Connection sub-tab for each camera.

Add goVision Recorders

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this video recorder is assigned to.
   b. Click [OK].
4. In the **Name** field, enter a unique, descriptive name for the video recorder.
5. Select "goVision" from the **Video Recorder Type** drop-down.
6. On the Connection sub-tab:
   a. Enter the workstation the video recorder connects to.
   b. Do one of the following:
      - Select the **Use IP Address of Video Recorder** radio button and enter an IP address.
      - Select the **Use Computer Name of Video Recorder** radio button and enter the computer's name.
   c. Enter the user name and password if desired. For more information, refer to LNVR Security and Passwords on page 925.
   d. Click [Detect] to connect to the recorder and verify the recorder type.
   e. Select the world time zone for the selected video recorder's geographical location.
   f. Select the **Daylight Savings** check box if you want to properly convert between various time formats for Daylight Saving Time.
   g. If desired, select the **Automatic clock synchronization** check box to automatically update the time.
7. Click [OK].
8. The Monitor Zone Assignments dialog is displayed. Select the monitor zone(s) you wish to assign the video recorder to and click [OK].

Add LDVR, Generic Video, or Loronix Video Recorders

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this video recorder is assigned to.
   b. Click [OK].
4. In the **Name** field, type a unique, descriptive name for the video recorder.
5. Select a video recorder type from the drop-down.
6. On the Connection sub-tab:

a. Enter the workstation the video recorder connects to.
b. Do one of the following:
   - Select the **Use IP Address of Video Recorder** radio button and enter an IP address.
   - Select the **Use Computer Name of Video Recorder** radio button and enter the computer's name.
c. Click [Detect] to connect to the video recorder to verify the recorder type.
d. Select the world time zone for the selected video recorder's geographical location.
e. Select the **Daylight Savings** check box if you want to properly convert between various time formats for daylight savings.

7. On the Recording sub-tab:

Note: Skip this step if you are configuring a Generic Video or Loronix video recorder.

a. Select a video standard from the drop-down.
b. For LDVR-408 and LDVR-444 recorders, select a video resolution from the drop-down.

8. On the Archiving/Purging sub-tab:

Note: Skip this step if you are configuring a Generic Video or Loronix video recorder.

a. Select an archive server and the timezone to archive, or leave the **Archive Server** field blank, if you do not want to archive video from the video recorder.
b. For LDVR-SP recorders:
   1) Select the **Enable Continuous Archiving** check box if you want video to be continually archived, 24 hours a day. Each camera must also be configured to archive continuously.
   2) Select the **Delay archiving until video buffer is less than __%** check box if you want the archive server to delay archiving until the video buffer is less than the specified amount. The recommended buffer size is 30%.
c. For LDVR-SP, LDVR-SP30, LDVR-408, and LDVR-444 recorders:
   1) Select the **Automatically Archive Video Events** check box if you want video events to be automatically archived or the **Automatically Purge Video Events** check box if you want video events to be automatically purged from the video recorder.
   2) For the **Threshold for Automated Archiving** spin buttons, choose the percentage of the video recorder disk space to be used by video events before automatic archiving begins.
   3) For the **Space to Automatically Free** spin buttons, choose the amount of disk space that should be freed up before the archiving or purging should stop.

9. Click [OK].
10. The Monitor Zone Assignments dialog is displayed. Select the monitor zone(s) you wish to assign the video recorder to and click [OK].

Notes: Before you use this video recorder, download your settings. To do this, right-click the video recorder in the video recorder listing window and select "Download".

Downloading is highly recommended even if the recorder appears to be in working order because it prevents the loss of configuration parameters.

Add NetDVMS Video Recorders

1. From the ***Video*** menu, select ***Digital Video***.

2. The Digital Video folder opens. Click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this video recorder is assigned to.
   b. Click [OK].
4. In the **Name** field, enter a unique, descriptive name for the video recorder.
5. Select "NetDVMS" from the **Video Recorder Type** drop-down.
6. On the Connection sub-tab:
   a. Enter the workstation the video recorder connects to.
   b. Do one of the following:
      - Select the **Use IP Address of Video Recorder** radio button and enter an IP address.
      - Select the **Use Computer Name of Video Recorder** radio button and enter the computer's name.
   c. Enter the user name and password if desired.
   d. Select the world time zone for the selected video recorder's geographical location.
   e. Select the **Daylight Savings** check box if you want to properly convert between various time formats for daylight savings.
7. If there is a external client configured on your system, you must configure it for the Send Video feature to work properly. On the Auxiliary Services tab.

Note: The external client must be added on the Auxiliary Services tab to appear in the drop-down. For more information, refer to Auxiliary Services Form on page 986.

8. Click [OK].
9. Import the NetDVMS configuration by right-clicking the NetDVMS in the listing window on the Video Recorder tab and selecting **Import From Recorder**. For more information, refer to Import Cameras Dialog on page 922.

IMPORTANT: Any time you add or remove a camera from the NetDVMS, the configuration will need to be updated manually in OnGuard. To do this, open the Administrator application on the master NetDVMS and close it without making changes. Then import the NetDVMS configuration from the Video Recorder tab in System Administration.

Configure Send Video with NetDVMS

Use this procedure to configure the Send Video feature on systems that do not have an external client.

1. Configure external client recipients on the master NetDVMS using the Administrator application. For more information, refer to the NetDVMS documentation.
2. Add the NetDVMS in System Administration. For more information, refer to Add NetDVMS Video Recorders on page 936.

Import IP Cameras from the Storage Calculator

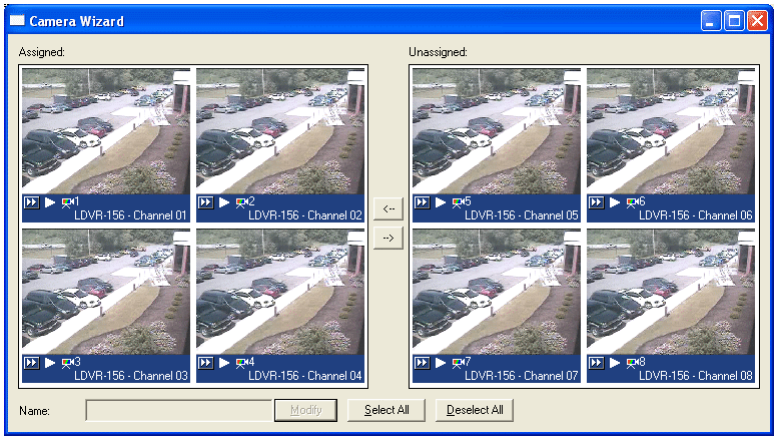
1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. On the Video Recorder form, right-click the LNVR recorder you wish to add the cameras to and select Import.
3. Browse for the configuration file (.xml). Select it and click [Open].

4. The IPCamera Wizard is displayed with a list including each of the cameras configured in the file. Change the Name, Input, IP Address, User Name, Password, Number of cameras and Online status as desired by clicking on the field in the listing window.
5. Select (place a check mark beside) each camera that you wish to add to the LNVR.
6. Click [Add] to add the selected cameras.

Add Multiple LDVR Cameras

Multiple LDVR cameras can be added simultaneously using the Camera Wizard from the Video Recorder form.

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. On the Video Recorder form, right-click an LDVR recorder and select Camera Wizard.
3. The Camera Wizard is displayed. The Unassigned window displays all available camera channels that have not yet been configured in the system. Select cameras from the Unassigned window with the mouse or by clicking the [Select All] button.



4. Click the [<--] arrow to add the selected unassigned cameras to the system and move them to the Assigned window. Cameras are named in the format *Recorder name - Channel number*.

Note: The Camera Wizard can be used to change the assigned name of a single selected camera by renaming it in the **Name** field and clicking [Modify].

5. When finished adding cameras, close the window.

Enter Notes for a Video Recorder

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Camera Form

Analog cameras are video cameras that require a video capture card to convert video to a digital signal, and require a PC to connect to the network.

IP Cameras

IP cameras are digital video cameras that connect directly to the network with their own IP address. IP cameras have the ability to transmit images using standard communication protocols such as TCP/IP. These cameras do not need to be connected to a PC or a video capture card. More advanced IP cameras may provide additional functionality such as a built-in web server, motion detection, alarm inputs/outputs, and e-mail and FTP support. IP cameras have a secure mode which can be enabled via the camera web page. With most cameras, this mode can be activated by changing the password for the root account and adding an additional account.

Camera Form - Common Form Elements Fields

Listing window

Lists currently defined cameras.

Name

A descriptive name for the camera. This is a “friendly” name assigned to each camera to make it easy to identify. Each name must be unique and contain no more than 32 characters.

Online

For cameras configured with LNVR and LDVR only. Select this check box to place the camera online. If you need to perform maintenance or replace a camera, deselect this check box.

When the **Online** check box is deselected:

- Video recorder stops recording and stops processing images for the specified camera
- Any requests to connect to the specified camera will receive an offline status
- Any requests for live video are denied
- If a failover recorder is configured, it will not record video for the specified camera

The ability to place a camera offline will be based on user privileges, and for LNVR, username and password.

Recorder

The video recorder that this camera communicates with.

Recorder Web Page

Opens the selected camera’s recorder configuration Web page where you can modify settings for the recorder. This button displays when you configure goVision recorders and OAAP recorders that support this feature.

Video Preview

Displays video from the camera for configuration purposes when the **Display Video** check box is selected.

Display Video

Select this check box to enable a preview of the camera video. When “(Failover Recorder)” is appended to this check box label, it indicates that the source of the video is the secondary recorder.

Add
Create a new camera entry.

Modify
Enables changes to be made to the selected camera entry.

Delete
Removes the selected camera entry.

Apply
Modifies the selected camera entry without exiting Modify mode.

Help
Displays online help for this topic.

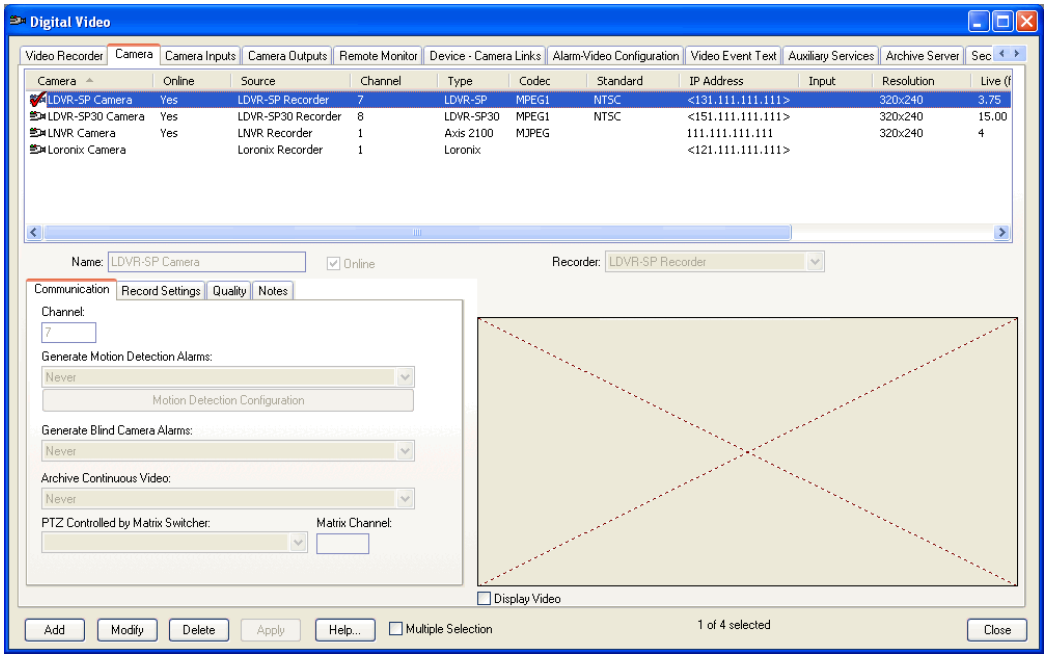
Multiple Selection
Select this check box to select multiple entries in the listing window.

Close
Closes the Digital Video folder.

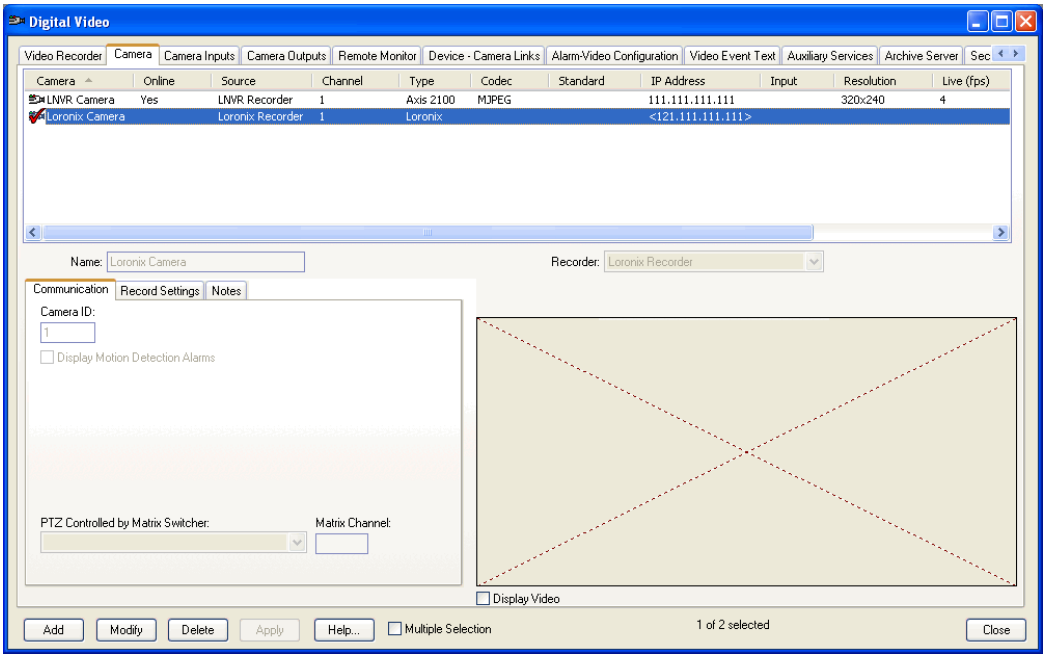
Camera Form (Communication Sub-tab)

The following Communication sub-tab displays if you configure a camera with an LDVR-SP, LDVR-SP30, LDVR-408, or LDVR-444 recorder.

Note: The **Generate Blind Camera Alarms** drop-down does not display for the LDVR-408 recorder and the **Archive Continuous Video** drop-down does not display for the LDVR-SP30, LDVR-408, or LDVR-444 recorder.



The following Communication sub-tab displays if you configure a camera with a NetDVMS, Generic Video or Loronix recorder.



Archive Continuous Video

Select the timezone in which video will be continuously archived for this camera. Video will only be archived during the selected timezone. The selected camera's video recorder must also be configured for continuous archiving.

Camera ID

An ID number for this camera.

Camera Type

If you are working with an LNVR video recorder, select a camera type. Choices include camera types that the selected video recorder supports.

Channel

The input channel number the camera connects to. Each camera must have its own unique channel.

LNVR recorders automatically assign the channel number, while other video recorders require user input.

Display Motion Detection Alarms

Select this check box if you want an alarm displayed in Alarm Monitoring when the camera detects motion.

Generate Motion Detection Alarms

Select a timezone from the drop-down if you want the camera to generate an alarm when motion is detected, during the selected timezone. Motion Detection is always on for cameras configured with LDVR recorders. Alarms will be generated only during the selected timezone. If you are using time-lapse mode, recording will jump to continuous mode whenever motion is detected

regardless of the selected timezone. The motion detection feature applies to cameras configured with LNVR, LDVR-SP, LDVR-SP30, LDVR-408, and LDVR-444 recorders.

- For LDVR-SP, LDVR-SP30,LDVR-408, and LDVR-444 recorders, the timezone for motion detection is set using this drop-down.
- For LNVR recorders, the timezone, frame rate, and threshold for motion detection are configured on the Video Processing form.

Generate Blind Camera Alarms

Select a timezone from the drop-down if you want the camera to generate an alarm when the blind camera threshold limit is reached, during the selected timezone. The blind camera feature may work differently for automatic gain control cameras. The blind camera feature applies to cameras configured with LNVR, LDVR-SP, LDVR-SP30, and LDVR-444 recorders.

- For LDVR-SP, LDVR-SP30, and LDVR-444 recorders, the timezone for blind camera detection is set using this drop-down.
- For LNVR recorders, the timezone, frame rate, and threshold for blind camera detection is configured on the Video Processing form.

Input Number

Enter an input number (1-4). This field is only available for Axis 2400 (NTSC) and (PAL) camera types associated with an LNVR video recorder.

Matrix Channel

The matrix input channel number the camera connects to.

- **Virtual matrix switchers** - When a camera is linked to a virtual matrix switcher in OnGuard, you should enter the drop-in address instead of a channel number in the **Matrix Channel** field. This address needs to match the address set on the camera via a dip switch.
- **Multi-drop with virtual matrix switchers** - When multi-drop is used the drop-in address for an RS-232 connection is always 1. Note that only RS-485 and RS-422 standards support multi-drop.

Motion Detection Configuration

Opens the Motion Detection Configuration window where you set the motion sensitivity and mask motion. For more information, refer to Configure Motion Detection and Apply Motion Mask to a Camera on page 967.

The motion detection feature applies to cameras configured with LNVR, LDVR-SP, LDVR-SP30, LDVR-408 and LDVR-444 recorders.

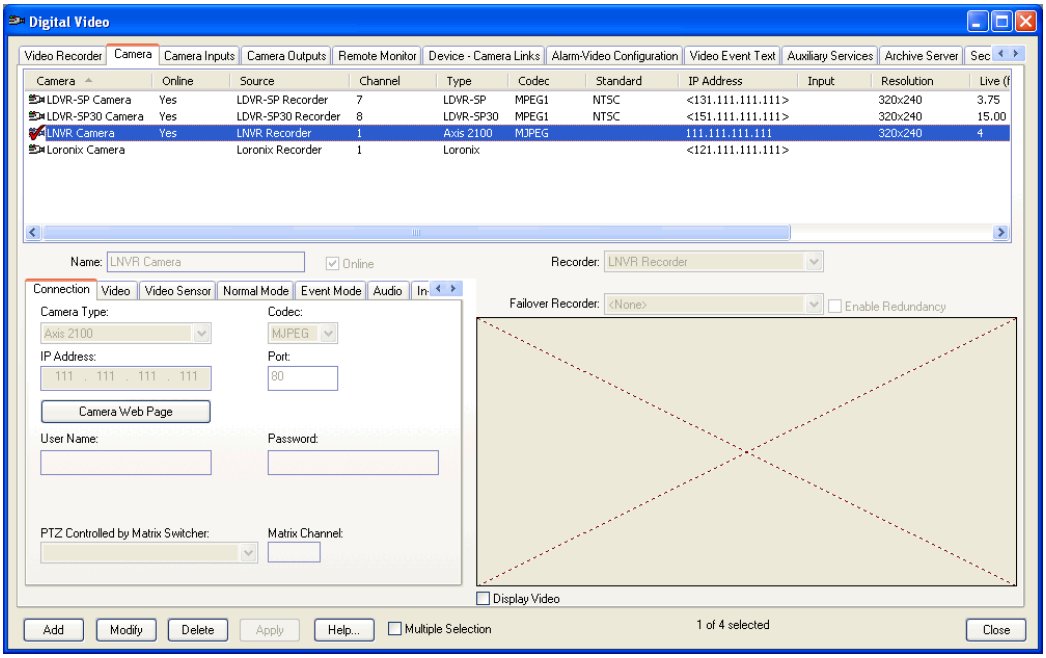
- For LDVR-SP, LDVR-SP30,LDVR-408, and LDVR-444 recorders, click the [Motion Detection Configuration] button.
- For LNVR recorders, motion detection is configured on the Video Processing form.

PTZ Controlled by Matrix Switcher

If the selected camera connects to a matrix switcher, choose the switcher from the drop-down. This field does not display when you configure a camera with an LNVR video recorder.

Camera Form (Connection Sub-tab)

The following Connection sub-tab displays if you configure a camera with an LNVR, goVision, or OAAP recorder. Different fields display depending on the capabilities of the video recorder and camera selected.



Camera Type

If you are working with an LNVR video recorder, select a camera type. Choices include camera types that the selected video recorder supports.

Camera Web Page

Opens the selected IP camera's configuration Web page where you can modify camera settings and view a camera's video output. For configuration procedures using a camera's web page, refer to the Digital Video Hardware User Guide. This button displays when you configure certain camera types.

Channel

The input channel number the camera connects to. Each camera must be on its own unique channel. This field displays when you configure certain camera types with a goVision or OAAP video recorder.

Codec

The compression type of the camera.

Failover Recorder

A failover/secondary recorder. For the selected channel, the failover recorder creates a virtual channel with the same settings as the original/primary recorder. If the original recorder is offline for a specific amount of time, an alarm is generated and the failover recorder begins recording video. When the primary recorder comes back online, it connects to the IP camera and resumes recording. The primary and failover recorders must share the same communication server. Only recorders that have the same communication server as the primary will appear in the **Failover Recorder** drop-down. For more information, refer to Video Recorder Failover and Redundancy on page 920.

Enable Redundancy

When a **Failover Recorder** is specified, this check box may be selected to activate the redundancy feature. This feature enables full-time failover mode, where the video channel records continuously to both the primary and failover recorders.

Generate Motion Detection Alarms

Select a timezone from the drop-down if you want the camera to generate an alarm when motion is detected, during the selected timezone. The motion detection feature applies to cameras configured with LNVR, LDVR-SP, LDVR-SP30, LDVR-408, and LDVR-444 recorders.

- For LDVR-SP, LDVR-SP30,LDVR-408, and LDVR-444 recorders, the timezone for motion detection is set using this drop-down.
- For LNVR recorders, the timezone, frame rate, and threshold for motion detection are configured on the Video Processing form.

IP Address

The IP address of the camera.

Port

A communication pathway from the video recorder to the camera. The default setting is an HTTP port setting, 80.

Standard

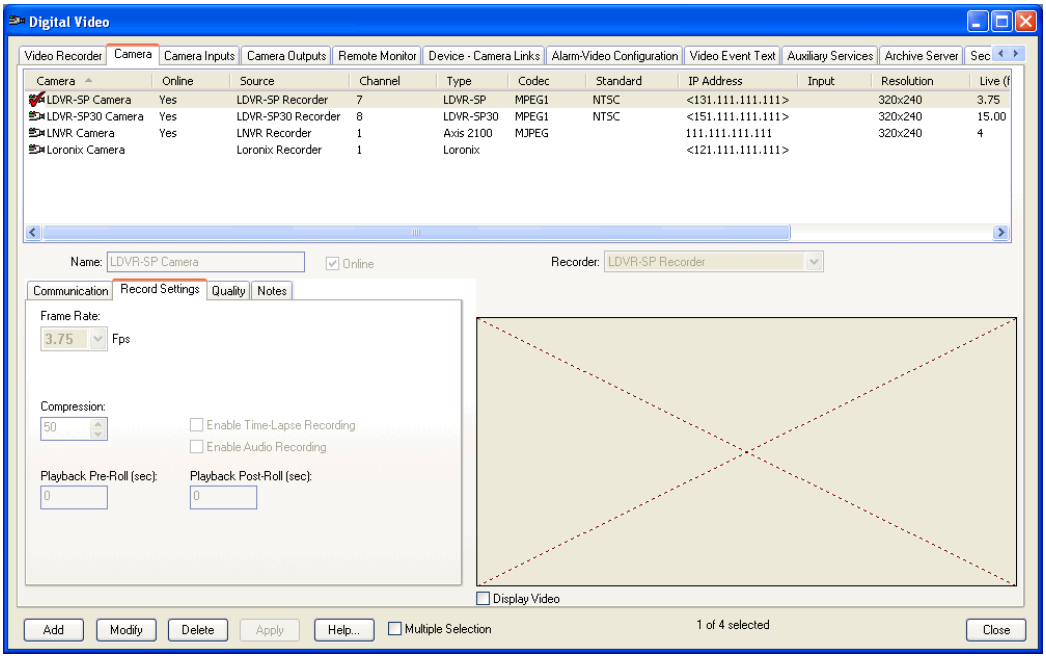
Select a video standard from the drop-down. This field displays when you configure certain camera types with an LNVR video recorder.

User Name/Password

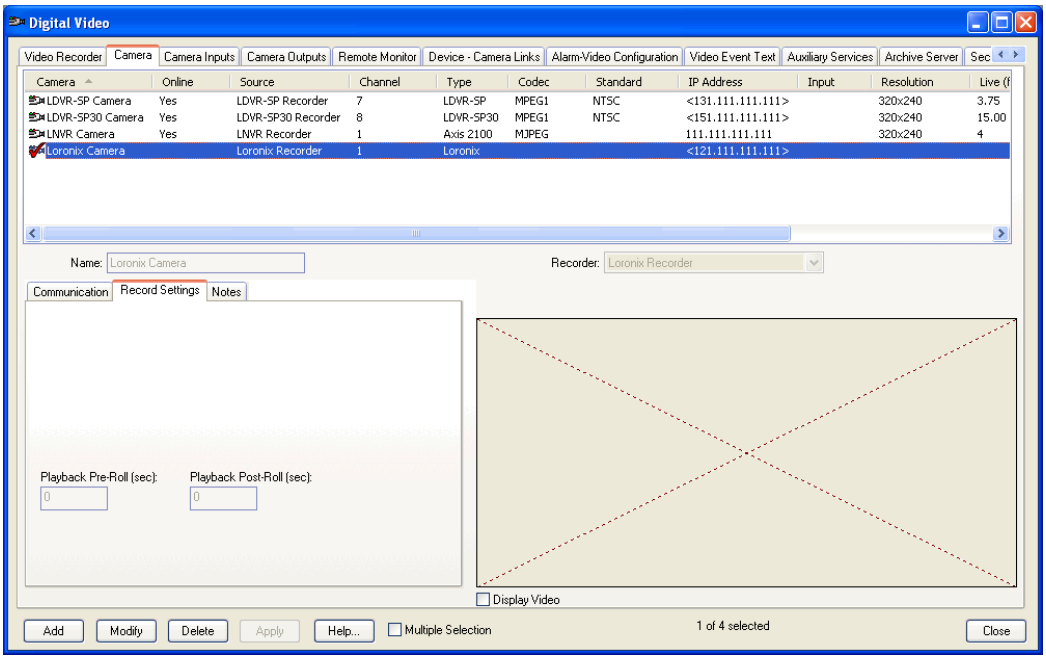
If the camera is configured to require authentication, then enter the valid username/password. Otherwise, leave these fields blank. Cameras are usually configured to require authentication on the camera's website.

Camera Form (Record Settings Sub-tab)

The following Record Settings sub-tab displays if you configure a camera with an LDVR-SP, LDVR-SP30, LDVR-408, or LDVR-444, recorder.



The following Record Settings form displays if you configure a camera with a NetDVMS, Generic Video or Loronix recorder.



Frame Rate

For cameras with LDVR-SP, LDVR-SP30, LDVR-408,or LDVR-444 video recorders:

- You can choose one of 5 different frame rates. The choices available in the drop-down depend on the recorder's current video standard (configured on the Video Recorder form).
- When there are no cameras defined, the default frame rate for a new camera is 3.7 fps (3.1 for PAL).

- When at least one camera is defined, the default frame rate for a new camera will be the frame rate of the camera that was selected just prior to adding the current camera.
- For LDVR-SP video recorders only, OnGuard regulates the frame rate automatically so that within each group of eight cameras (cameras 1 through 8, cameras 8 through 16, etc.) the sum of the frame rates does not exceed 30 fps (25 for PAL).
- If the camera is in time-lapse mode, the frame rate must be 3.75 fps or higher.

Compression

The amount of compression to use while recording an event. Compression effects video quality and is dependent on the video frame rate.

Enable Time-Lapse Recording

Select this check box if you want the frame rate for the selected video recorder to be lower when no motion is detected. The lower frame rate is called the *Non-Motion Frame Rate*. Time-lapse recording must also be enabled for the recorder, otherwise the state of this check box is ignored and video is constantly recorded at the frame rate configured in the **Frame Rate** drop-down. Time-lapse recording is enabled for the recorder on the Recording sub-tab of the Video Recorder form.

When the camera is in time-lapse mode, the value entered in the **Frame Rate** field must be 3.75 or higher if the recorder is configured for NTSC (3.1 or higher if the recorder is configured for PAL). Motion Detection is always on for cameras configured with LDVR-SP, LDVR-SP30, LDVR-408,or LDVR-444 video recorders. Whenever motion is detected, the camera will switch to continuous recording mode.

Enable Audio Recording

Select this check box if you want to enable audio recording for live and recorded video. Audio recording can be enabled for each camera.

Pre-Roll

The *pre-roll* is the number of seconds automatically subtracted from the start time of alarms/events generated by this camera to ensure that the video associated with the event includes footage prior to the actual event. For example, if a criminal disables a camera before executing a crime, the pre-roll greatly increases the odds that a video event includes footage of the criminal disabling that camera.

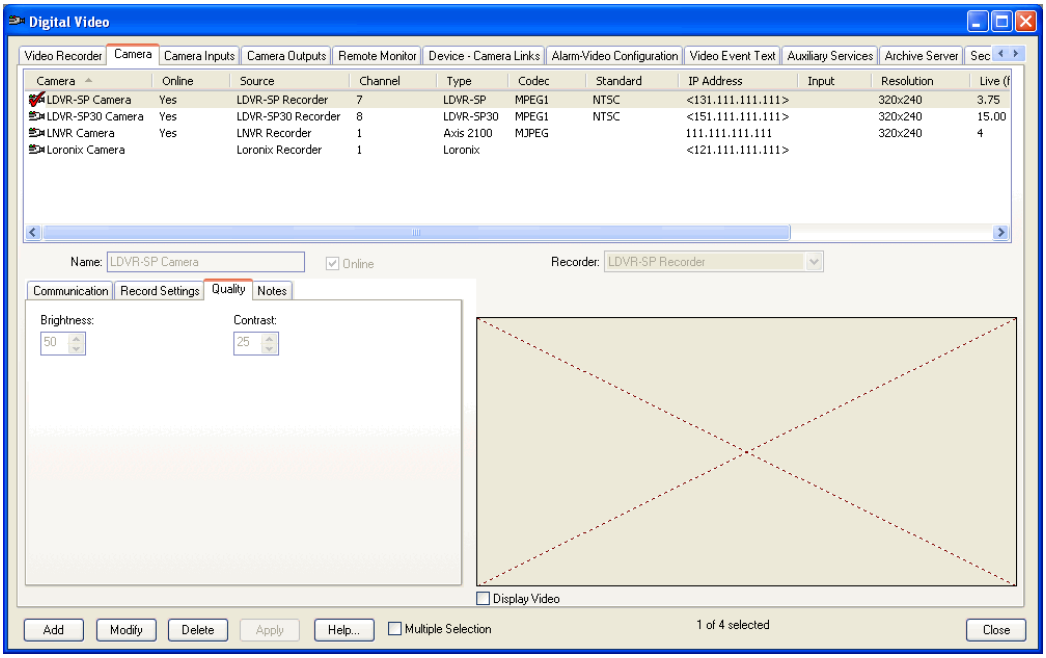
Post Roll

The *post roll* is the number of seconds automatically added to the end time of alarms/events generated by this camera to ensure that the video associated with the event includes footage following the actual event.

Camera Form (Quality Sub-tab)

Note: The Quality sub-tab does not display if you configure a camera with a Generic Video recorder, LNVR, or Loronix recorder.

The following Quality tab displays if you configure a camera with an LDVR-SP, LDVR-SP30, LDVR-408, or LDVR-444 recorder.



Brightness

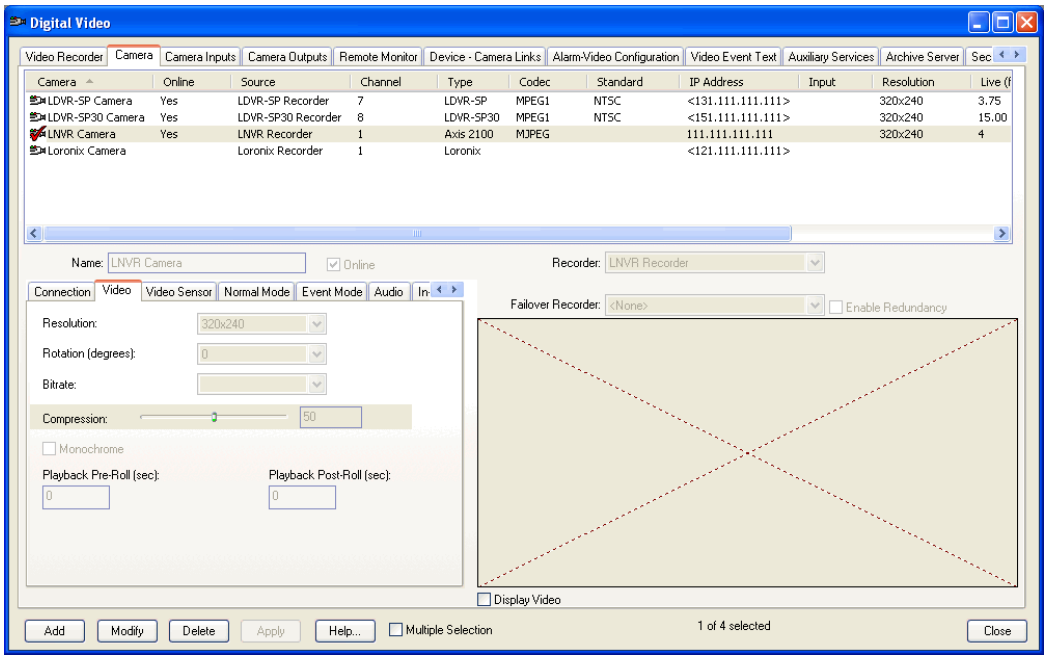
The camera's brightness level. High values increase the difference between the image's brightest and darkest elements.

Contrast

The camera's contrast level. By adjusting the contrast level you can increase or decrease the range of gray contained in the image, as well as increase or decrease the distinction between the lightest and darkest tones in the image.High contrast values make light areas lighter and dark areas darker.

Camera Form (Video Sub-tab)

The following Video form displays if you configure a camera with an LNVR, goVision, or OAAP recorder. Different fields are available depending on the type of camera selected.



Auto

Select the check box if you want to accept the default (auto) settings.

Compression

The amount of compression to use while recording an event. Compression effects video quality and is dependent on the video frame rate.

Bitrate

The physical space (in bits not bytes) one second of audio or video requires.

Monochrome

Select this check box if you want to record video in monochrome (black and white). The **Monochrome** check box does not display for the Sony camera types and the Axis 2100,2120, 2420 (NTSC and PAL) camera types.

Playback Post-Roll (sec)

The *post-roll* is the number of seconds automatically added to the end time of alarms/events, generated by a camera, to ensure that video associated with the event includes footage of the scene after the actual event.

Playback Pre-Roll (sec)

The *pre-roll* is the number of seconds automatically subtracted from the start time of alarms/ events, generated by a camera, to ensure that video associated with the event includes footage prior to the actual event. For example, if a criminal disables a camera before executing a crime, the pre-roll greatly increases the odds that a video event includes footage of the criminal disabling that camera.

Resolution

The image resolution (number of pixels across and down).

Rotation (degrees)

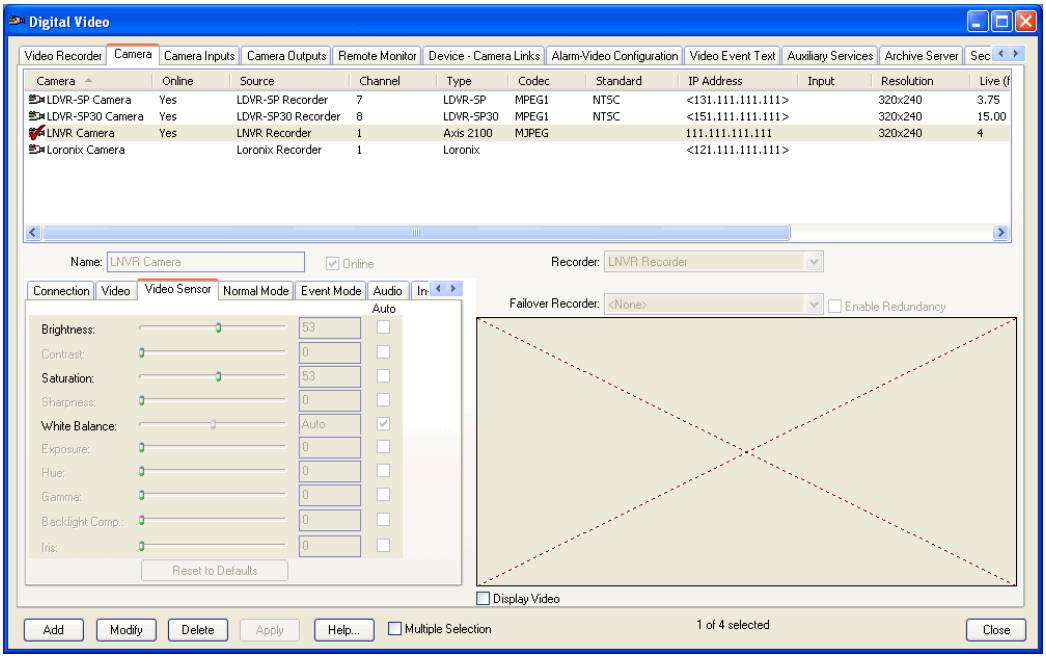
The degrees of rotation for the camera view. The image is rotated clockwise as the value increases. For PTZ cameras, see the section on Rotation for PTZ Cameras on page 949.

Rotation for PTZ Cameras

In most cases, PTZ cameras are designed for ceiling mount. The camera web page should be configured to indicate ceiling mount or 0° rotation. If the camera is not designed for ceiling mount, the rotation may need to be adjusted on the camera web page. Any rotation adjustments for the placement of the camera should be configured through the OnGuard software. Failure to configure PTZ rotation correctly may cause unpredictable PTZ control.

Camera Form (Video Sensor Sub-tab)

The following Video Sensor form displays if you configure a camera with a LNVR, goVision, or OAAP recorder. Different fields are available depending on the type of camera selected.



Auto

Select the check box if you want to accept the default (auto) settings.

Default

Resets all video sensor fields to the default values.

Brightness

The camera's brightness level. High values increase the difference between the image's brightest and darkest elements. Select the check box if you want to accept the default (auto) settings.

Contrast

The camera's contrast level. By adjusting the contrast level you can increase or decrease the range of gray contained in the image, as well as increase or decrease the distinction between the lightest and darkest tones in the image.High contrast values make light areas lighter and dark areas darker. Select the check box if you want to accept the default (auto) settings.

Saturation

The camera's saturation level. Adjusting the saturation level adjusts the purity of color (the number of colors used to create a particular color). Higher values increase the saturation (purity); lower values decrease saturation. Select the check box if you want to accept the default (auto) settings.

Sharpness

The camera's sharpness level (how focused or blurry the image is). Select the check box if you want to accept the default (auto) settings.

White Balance

The camera's white balance level. By adjusting the white balance you redistribute shades of colors. White balance makes the darkest color in the image black and the lightest color in the image white, and adjusts the colors in between. Select the check box if you want to accept the default (auto) settings.

Exposure

The camera's exposure level. High levels increase the amount of time light passes through the lens. Select the check box if you want to accept the default (auto) settings.

Hue

Hue perceptually, corresponds approximately to "color". Functionally, hue is a phase relationship of the chrominance components. Select the check box if you want to accept the default (auto) settings.

Gamma

Gamma is a measure of contrast in an image, typically in the midrange grays (mid-tones). Adjusting the gamma allows you to correct mid-tones without noticeable changes in the highlight and shadow areas. Gamma is also the way the brightness of an image is interpreted by computer hardware. Many IP Cameras let you adjust the gamma level to alter the image appearance or to compensate for brightness or color in a room. Select the check box if you want to accept the default (auto) settings.

Backlight Comp

Backlight compensation adjusts the light level of the background image. This setting is useful in situations when there is a difference in available light between the subject and the background. If the background has too much light, the subject tends to appear dark. In this situation, increase the backlight comp value to compensate. Select the check box if you want to accept the default (auto) settings.

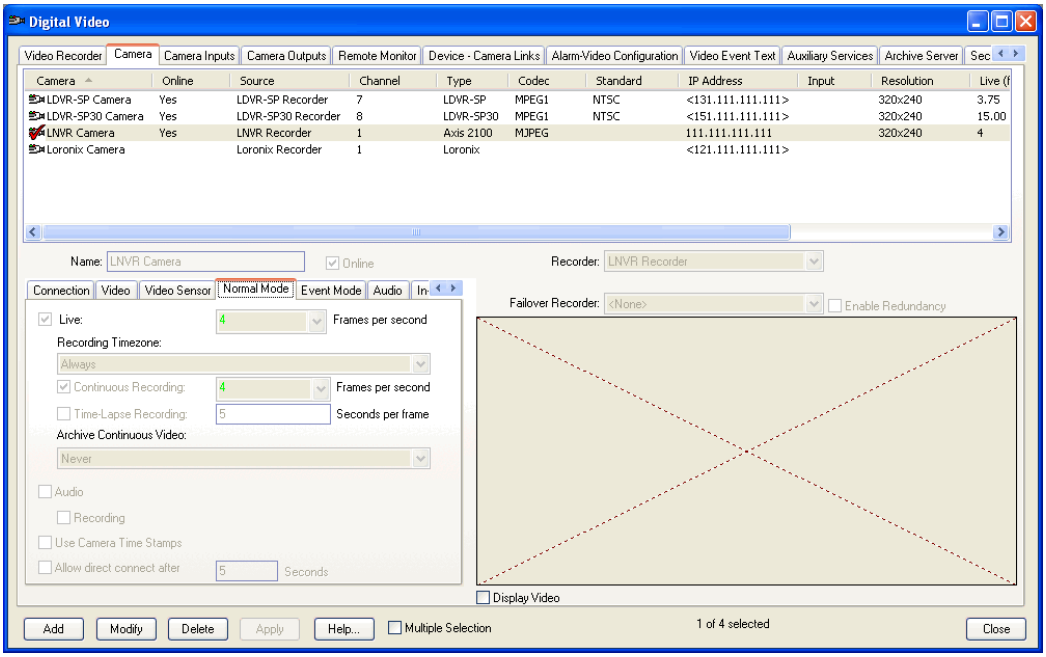
Iris

The iris adjusts the lens opening on the camera, which regulates the amount of light entering a camera. Select the check box if you want to accept the default (auto) settings.

Camera Form (Normal Mode Sub-tab)

Note: This sub-tab does not display when you configure a camera with a Generic Video, LDVR-SP, LDVR-SP30, LDVR-408, LDVR-444, or Loronix recorder.

The following Normal Mode sub-tab displays if you configure a camera with an LNVR, goVision, or OAAP recorder. Different fields display depending on the type of camera selected.



Live

The frame rate to view live video in Alarm Monitoring. If the selected value is within the recommended range, the value will be displayed in green, otherwise it will be displayed in red. The live recording value limits the options available for continuous recording and event recording.

For example, if you select 10 fps for live recording, then the continuous recording and event recording fields display values up to 10 fps. If you select 4 fps for live recording, then the options are limited to values up to 4 fps.

The **Live** check box must be selected to process video events. When live video capture is disabled, **Pre-Roll** is also disabled on the Event Mode sub-tab.

Recording Timezone

If you wish to limit recording to a specific timezone, select it from the drop-down. The default value is Always. If a timezone other than Always is selected, video will only be recorded during the selected timezone. For goVision recorders:

- "Always" sets the Cont HQ (Continuous High Quality) schedule to Daily from 00:00 to 24:00 on the recorder.
- "Never" disables Continuous High Quality recording on the recorder.
- "<Use Recorder Configuration>" uses the setting as it is configured on the goVision recorder.

Continuous Recording

Select this check box if you want video recorded constantly at the selected frame rate. If the selected value is within the recommended range, the value will be displayed in green, otherwise it will be displayed in red.

The values available in the drop-down are limited by the live frame rate. Refer to the definition for Live frame rate for more information.

Some codecs will allow you to record key frames only, which will record only the I-frames and none of the P-frames resulting in video compression.

For goVision recorders, the continuous recording frame rate sets the Continuous High Quality frame rate on the recorder.

This feature is not supported for LNVR cameras in H.264 mode. The LNVR can only record at the rate of live recording, not less. Due to the nature of the H.264 algorithm, the gains of such a configuration are not as necessary as they are with non-motion based encoding technologies such as MJPEG. The frames that would be dropped comprise an insignificant percentage of the total storage due to the encoding algorithm.

Time-Lapse Recording

Select this check box if you want the frame rate to be lower when there is no motion detected. When selected, enter a time-lapse recording rate. The range of values is 2 to 30 seconds per frame. This unit of measure (seconds per frame) implies all values are less than 1 frame per second. For example if you enter 2 seconds per frame, that is the equivalent of.5 frames per second.

For goVision recorders, if you set the time-lapse seconds per frame value to 2, 4, 8, or 16 seconds per frame, this will be set as 1/2 fps, 1/4 fps, 1/8 fps, or 1/16 fps respectively on the recorder.

MPEG4 cameras should be configured with a live frame rate of at least 12 fps when enabling time-lapse recording. Lower live frame rates, especially in combination with low seconds per frame time-lapse recording, can cause uneven gaps between frames and blocks of continuous recording between gaps.

This feature is not supported for LNVR cameras in H.264 mode. The LNVR can only record at the rate of live recording, not less. Due to the nature of the H.264 algorithm, the gains of such a configuration are not as necessary as they are with non-motion based encoding technologies such as MJPEG. The frames that would be dropped comprise an insignificant percentage of the total storage due to the encoding algorithm.

Archive Continuous Video

Select the timezone in which video will be continuously archived for this camera. Video will only be archived during the selected timezone. The selected camera's video recorder must also be configured for continuous archiving.

Audio

Select this check box to enable live audio.

Recording

Select this check box to enable audio recording. Audio is only recorded when video is also recording. With the In-Camera Storage feature it is not necessary to select the **Recording** check box. Recorded video will automatically include audio when the **Audio** check box is selected.

Use Camera Time Stamps

Select this check box to enable camera time stamps. The camera time must be synchronized with the LNVR prior to enabling this feature. For more information, refer to Camera Time Stamps on page 953.

Allow direct connect after ____ Seconds
Select this check box to allow a direct connection to the camera when the connection to the LNVR is lost. Specify the number of seconds before the direct connection is available.

Display Date
Select this check box if you want to display the date as an overlay.

The **Display Date** check box does not display for the Sony SNC-RZ30 PTZ (NTSC and PAL) camera type.

Display Time
Select this check box if you want to display the time as an overlay. The **Display Time** check box does not display for the Sony SNC-RZ30 PTZ (NTSC and PAL) camera type.

Display Title
Select this check box if you want to display the title as an overlay.

Camera Time Stamps

By default, time stamps are generated by the LNVR at the time the sample is received. This method may encounter inaccuracies across networks with bandwidth limitations and cause problems for features that require high accuracy such as IntelligentVideo.

A more reliable method uses time stamps generated by the camera. Prior to enabling the use of camera time stamps, the time on the camera and LNVR must be synchronized. The recommended method is through use of an NTP server. A third-party application can be used to synchronize the LNVR, and the camera web page can be configured to connect the camera to the NTP server. Both the camera and the LNVR must use the same NTP server.

Note: If the time difference between the camera time stamps and the time on the LNVR is greater than 20 seconds, the recorder time stamps will be used. The Camera Time Stamps feature cannot be used across different world time zones.

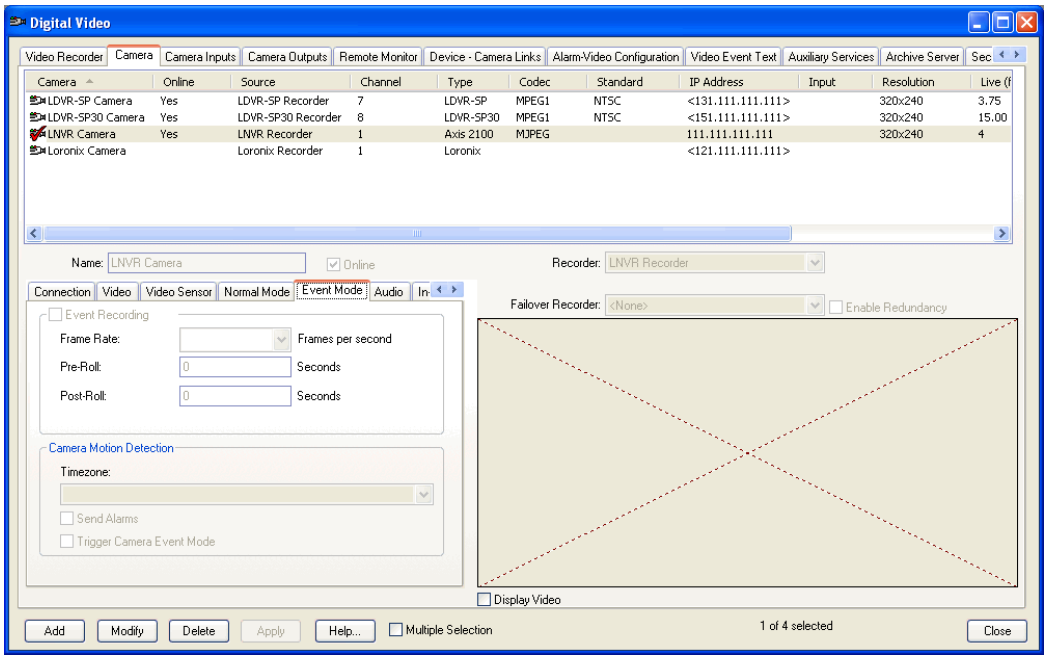
Camera Form (Event Mode Sub-tab)

The Event Mode sub-tab displays if you configure a camera with an LNVR, goVision, or OAAP recorder.

For special considerations with pre- and post-roll on goVision video recorders, refer to Pre- and Post-roll Considerations for goVision Recorders on page 955.

Event Mode Sub-tab Functions

- Increase frame rate with pre-roll time for OnGuard related events
- Enable OnGuard specific events to trigger event recording mode



Event Recording

Select this check box if you want to enable event recording for the selected camera. When selected you can configure the recording frame rate and pre-roll for an event. When the event is complete, non-event recording mode resumes. This feature is not supported for cameras in H.264 mode. The LNVR can only record at the rate of live recording. Due to the nature of the H.264 algorithm, the gains of such a configuration are not as necessary as they are with non-motion based encoding technologies such as MJPEG.

Frame Rate

Select the frame rate for event recording mode. If the selected value is within the recommended range, the value will be displayed in green, otherwise it will be displayed in red.

If using MJPEG, the values available in the drop-down are limited by the live frame rate value on the Normal Mode sub-tab. For example, if you select 10 fps for live recording (on the Normal Mode sub-tab), then the event recording frame rate displays values up to 10 fps. If you select 4 fps for live recording, then the event recording is limited to values up to 4 fps. If using H264 or MPEG4, if you select 10 fps for live recording then the event recording frame rate displays two values: 10 fps and Key Frame Only.

Some codecs will allow you to record key frames only, which will record only the I-frames and none of the P-frames resulting in video compression.

Pre-Roll

The pre-roll is the number of seconds automatically subtracted from the start time of alarms/events, generated by this camera, to ensure that the video associated with the event includes footage prior to the actual event (at the event recording frame rate).

For example, if a criminal disables a camera before executing a crime, the pre-roll greatly increases the odds that a video event includes footage of the criminal disabling that camera.

Typically the playback pre-roll does not need a value greater than 30 seconds, however for special circumstances it can be configured to up to 900 seconds. Pre-roll video is buffered in the system memory, and setting a high value for this field cause a large increase on the amount of system resources used. For more information, refer to Estimate RAM Needed for Pre-roll on page 966.

For special considerations with pre- and post-roll on goVision video recorders, refer to Pre- and Post-roll Considerations for goVision Recorders on page 955.

Post-Roll

The *post-roll* is the number of seconds automatically added to the end time of alarms/events generated by this camera to ensure that the video associated with the event includes footage following the actual event. For special considerations with pre- and post-roll on goVision video recorders, refer to Pre- and Post-roll Considerations for goVision Recorders on page 955.

Timezone

Select the access control timezone during which you wish to activate camera motion detection.

For goVision recorders:

- "Always" sets the Cont HQ (Continuous High Quality) schedule to Daily from 00:00 to 24:00 on the recorder.
- "Never" disables Continuous High Quality recording on the recorder.
- "<Use Recorder Configuration>" uses the setting as it is configured on the goVision recorder.

Send Alarms

Select this check box to send alarms to Alarm Monitoring.

Trigger Camera Event Mode

Select this check box to activate the camera's event recording mode upon an event.

Configure

Click this button to launch the Hybrid Card VMD Configuration Utility to configure regions of interest for the camera channel. This button will only be displayed for Lenel DS4016HCl hybrid camera channels.

Pre- and Post-roll Considerations for goVision Recorders

On goVision recorders, the event recording Pre-Roll value sets the Pre-Event Recording on the video recorder, and the Post-Roll value sets the Post-Event Recording value on the video recorder. OnGuard offers greater granularity when setting the pre- and post-roll values and these must be converted when setting the values on the goVision recorder. The following tables describes how the OnGuard setting will be set on the goVision recorder.

Pre-roll Setting Conversion for goVision

OnGuard Pre-roll	goVision Pre-event Recording
0	None
1-5 seconds	5 seconds
6-10 seconds	10 seconds
11-15 seconds	15 seconds
16-20 seconds	20 seconds
21-25 seconds	25 seconds
26-30 seconds	30 seconds

Pre-roll (Continued)Setting Conversion for goVision

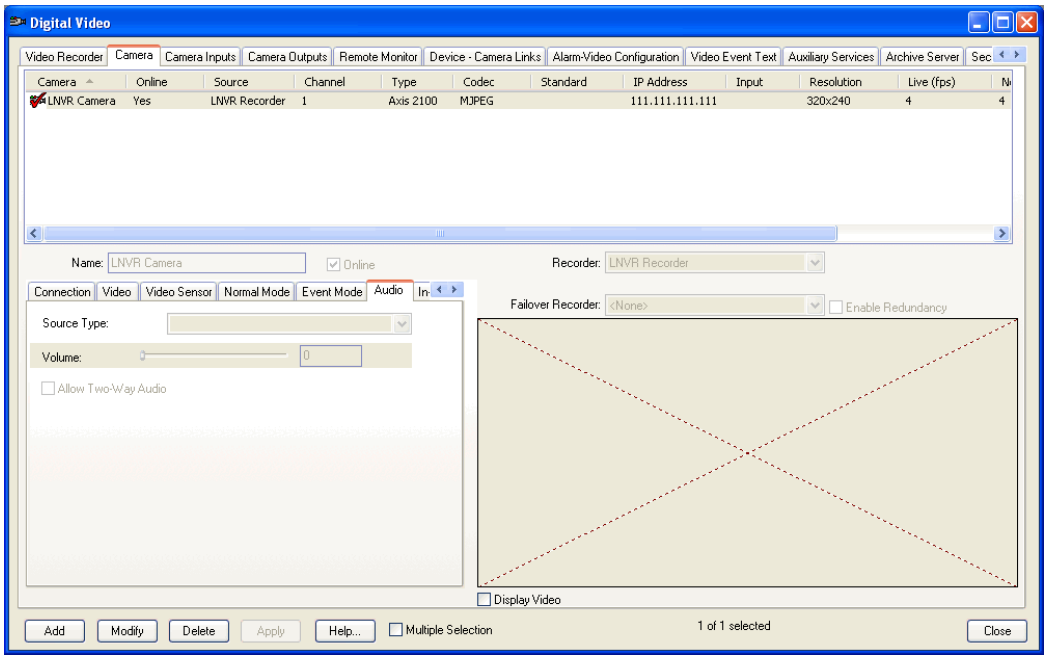
OnGuard Pre-roll	goVision Pre-event Recording
> 30 seconds	MaxPreRecord

Post-roll Setting Conversion for goVision

OnGuard Post-roll	goVision Post-event Recording
0-5 seconds	5 seconds
6-10 seconds	10 seconds
11-30 seconds	30 seconds
31-60 seconds	1 minute
61-120 seconds	2 minutes
121-300 seconds	5 minutes
301-600 seconds	10 minutes

Camera Form (Audio Sub-tab)

The following Audio sub-tab displays if you configure a camera with an LNVR, goVision, or OAAP recorder.



Source type
Select the source type from the drop-down. Options available reflect individual camera capabilities. Refer to the camera manufacturer's manual for information about available audio source types. This field is not required for some camera types.

Volume
Use the slider or enter a number into the text box to set the volume.

Allow Two-Way Audio
Select this check box to enable Two-Way Audio for the selected camera. If Two-Way Audio is not supported for the camera this check box will be grayed out.

Camera Form (In-Camera Storage Sub-tab)

The In-Camera Storage feature allows video to be stored in the memory of a remote camera for later retrieval and storage in the LNVR. This feature is designed to facilitate systems that may experience high bandwidth during specific parts of the day, thus delaying the transfer of video to the LNVR until non-peak hours.

Continuous recording is not supported with In-Camera Storage. Due to the limited amount of memory within the camera, motion detection or camera inputs should be employed to only record events. Motion Detection sensitivity should be set such that only meaningful events are recorded.

Live video playback places considerable strain on the camera. The camera will appear offline in Alarm Monitoring. When requesting live video, there is a delay while the server establishes the initial connection to the camera for the transfer. Current IP camera technology, at the time of this release, may experience jumps or choppiness during live video playback.

If recorded video is requested that has not yet been retrieved from the camera, it will be downloaded to the LNVR and temporarily stored for playback. There will be a delay while the video is downloaded to the LNVR. If only a portion of the requested video has been retrieved, only the portion already stored on the LNVR will be played back. An additional request must be made for the video still stored on the camera.

Camera Requirements

Cameras must support the following requirements to be used for this feature:

- Storage of video and audio events must be based on motion detection or external triggers events via camera inputs.
- The storage of video and audio is stored in the memory of the camera and can be retrieved via FTP. The FTP server is required to operate for the appropriate camera memory (internal or external).
- The camera needs to operate in MPEG4 mode with cropping set to off as required from Sony in order to record video.
- A list of supported cameras and features for each LNVR version can be found on the secure "customer self-service center" portion of the Lenel website: https://customer.lenel.com/?=node/66

Camera Configuration

The following steps must be performed via the camera web page to configure In-Camera Storage:

1. Set up the FTP server.
2. Configure the image memory with overwrite set to on.
3. Configure motion detection or external triggers.
4. Clear the camera memory.
5. Enable the Alarm Buffer and set the Alarm Buffer pre- and post-roll to at least 1 second.
6. Synchronize the time for the camera and LNVR.

Considerations for Several Sony Cameras

The following Sony cameras support the option for extended memory storage:

- Sony SNC-RZ25
- Sony SNC-RZ50
- Sony SNC-RX550
- Sony SNC-CS50
- Sony SNC-P5

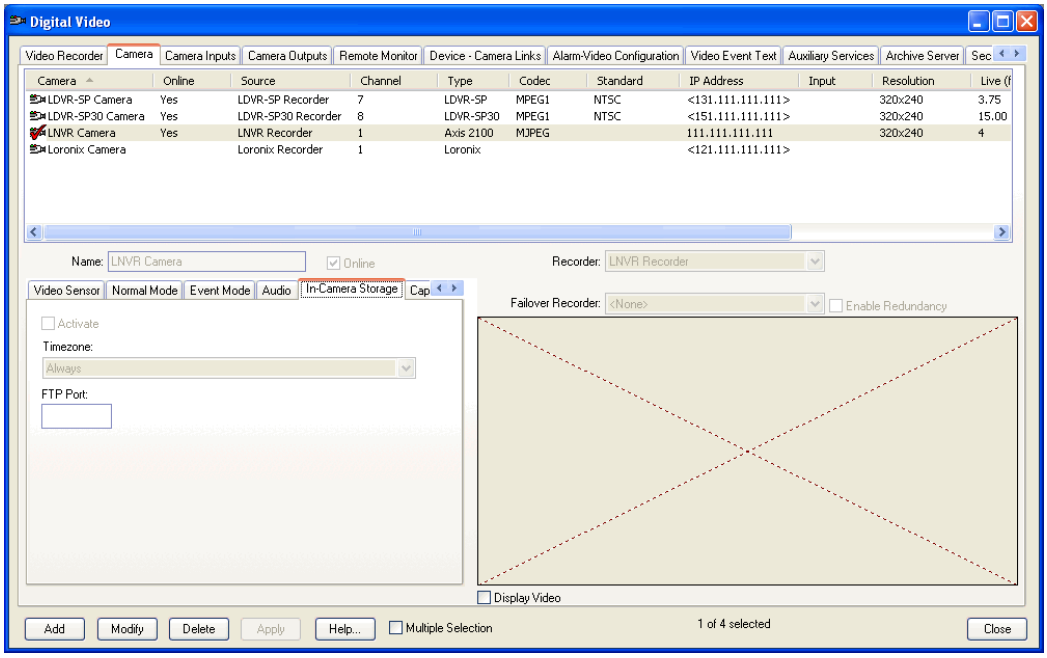
There are special configuration steps for these cameras:

- **Selected root directory** should be set to the same source for both the FTP server and image memory.
- Add-on module must be formatted using a PCMCIA adaptor to plug the unit into a laptop.
- PTZ Preset scheduling is not supported with In-Camera Storage.

Note: PTZ control may cause additional choppiness with live video due to the motion created by the camera movement.

Software Configuration

The following In-Camera Storage sub-tab displays if you configure a camera with an LNVR recorder. Different fields display depending on the type of camera selected.



Note: When enabling/disabling In-Camera Storage, any users currently accessing the system must log out then back in to Alarm Monitoring to use the new settings.

Camera Form - In-Camera Storage Sub-tab Fields

Activate

Select this check box to enable the In-Camera Storage feature. This feature will deactivate live and continuous recording and audio recording. Prior to enabling In-Camera Storage, the desired fps should be configured in the **Live** drop-down on the Normal Mode sub-tab.

Timezone

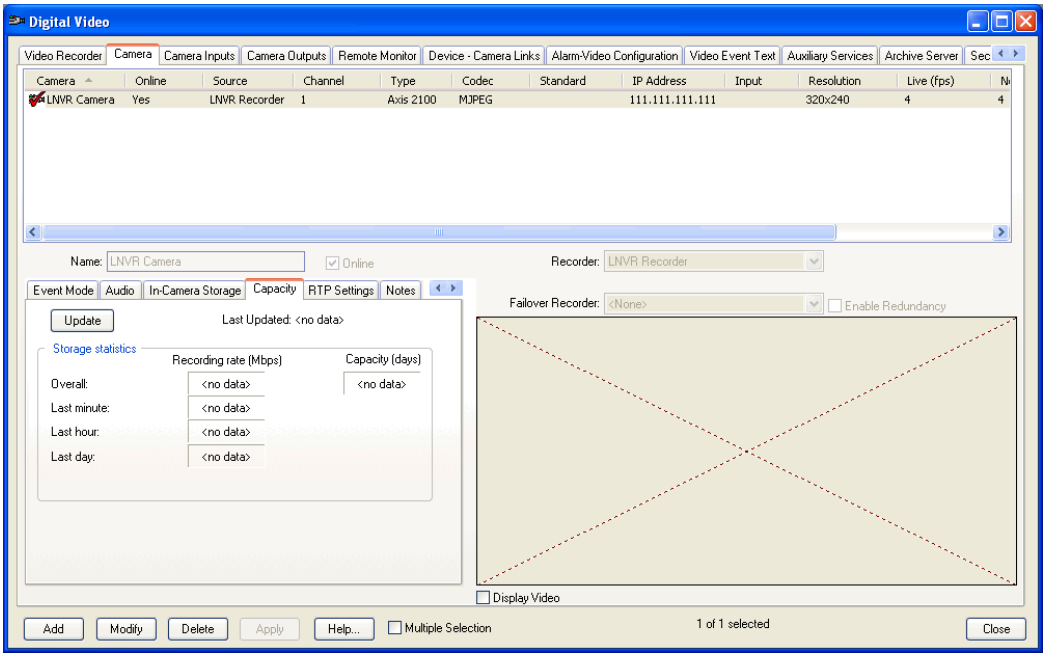
Select the access control timezone to retrieve recorded video from the camera. During the selected timezone, the LNVR will periodically connect to the camera to download recorded video.

FTP Port

Enter the number of the port on the camera that allows incoming connections to be set. The Sony factory default is 21.

Camera Form (Capacity Sub-tab)

The following Capacity sub-tab displays if you configure a camera with an LNVR recorder.



Update

Connects to the video recorder to retrieve the current storage statistics.

Overall

Displays the total average recording bit rate in Mbps. According to this rate, the recorder should be able to store the number of days worth of video listed in the Capacity (days) column.

Last minute
Displays the average recording bit rate in Mbps for the last minute.

Last hour
Displays the average recording bit rate in Mbps for the last hour.

Last day
Displays the average recording bit rate in Mbps for the last day.

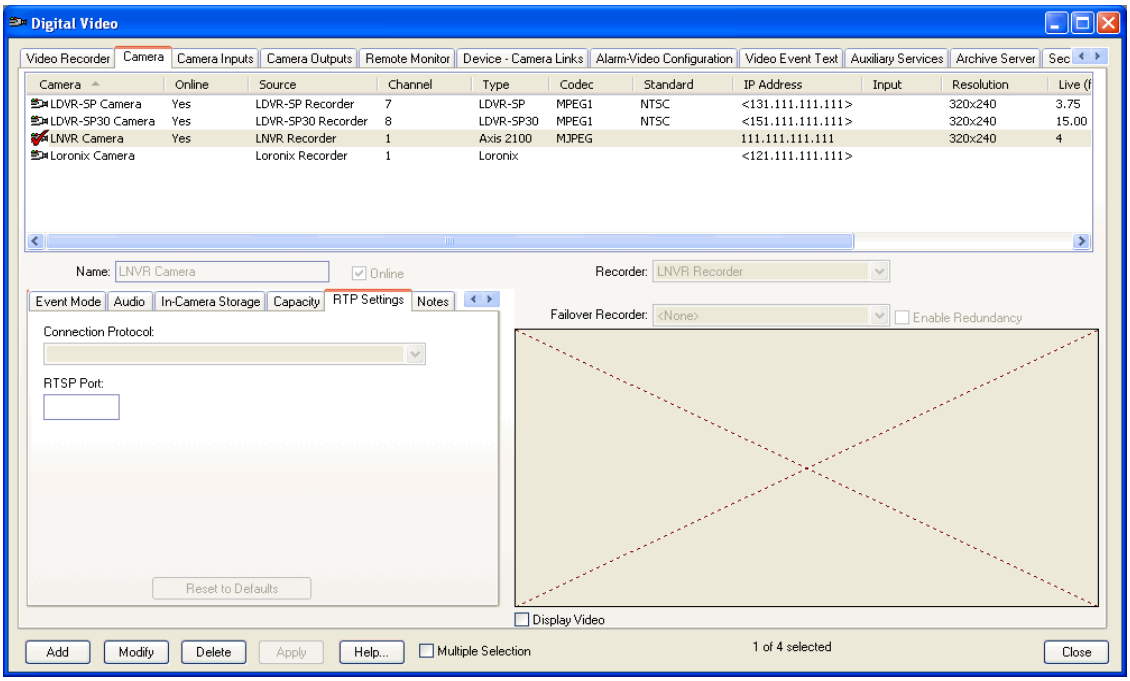
Capacity
Displays the amount of video currently stored on the video recorder.

Camera Form (RTP Settings Sub-tab)

Real-time Transport Protocol (RTP) is a standardized packet format for delivering video and audio over the Internet. RTP works in conjunction with RTSP protocol in OnGuard. RTP is used to transmit the data and RTSP is used to control video playback.

The RTP Settings sub-tab is used to configure the system to receive video from RTP-enabled cameras. Not all cameras support RTP/RTSP protocols. Of the cameras that do support RTP/RTSP, all of them support RTP via UDP/IP. Refer to the documentation provided with the camera to determine the connection type available. Only options supported by the camera will be available in the **Connection Protocol** drop-down.

The RTP Settings sub-tab displays if you configure a camera with an LNVR recorder.



Connection Protocol
The following options are supported by OnGuard. Only options supported by the camera will be available in the drop-down.

- **RTP via Multicast** is a multicast protocol used for video transmission. The advantage of multicast is that a single stream of data is sent across the network that multiple clients can share. Not all cameras support multicast.
- **RTP via UDP/IP** is a unicast protocol for video transmission. Each client that connects to the camera creates a stream of data that is sent across the network. The disadvantage of UDP/IP is that on a lossy network, you may experience a large number of missing frames resulting in poor video quality. Also, on some networks, routers or firewalls block UDP/IP transmissions.
- **RTP via RTSP** tunnels RTP protocol within RTSP protocol which is based in TCP/IP. This protocol does not use UDP/IP and transmits all streams through one TCP/IP port. Transmission is reliable and lost packets are retransmitted. The disadvantage is a larger amount of network traffic over UDP/IP. On a well-configured network, lost packets should not be an issue, making tunneling and using TCP/IP more expensive than using UDP/IP.
- **RTP via RTSP via HTTP** tunnels RTP within RTSP but is then tunneled through HTTP. This protocol is less efficient than RTP via RTSP, however the video and session control are transmitted over HTTP using TCP/IP port 80, often requiring no changes in a firewall configuration if present between the recorder and the camera.

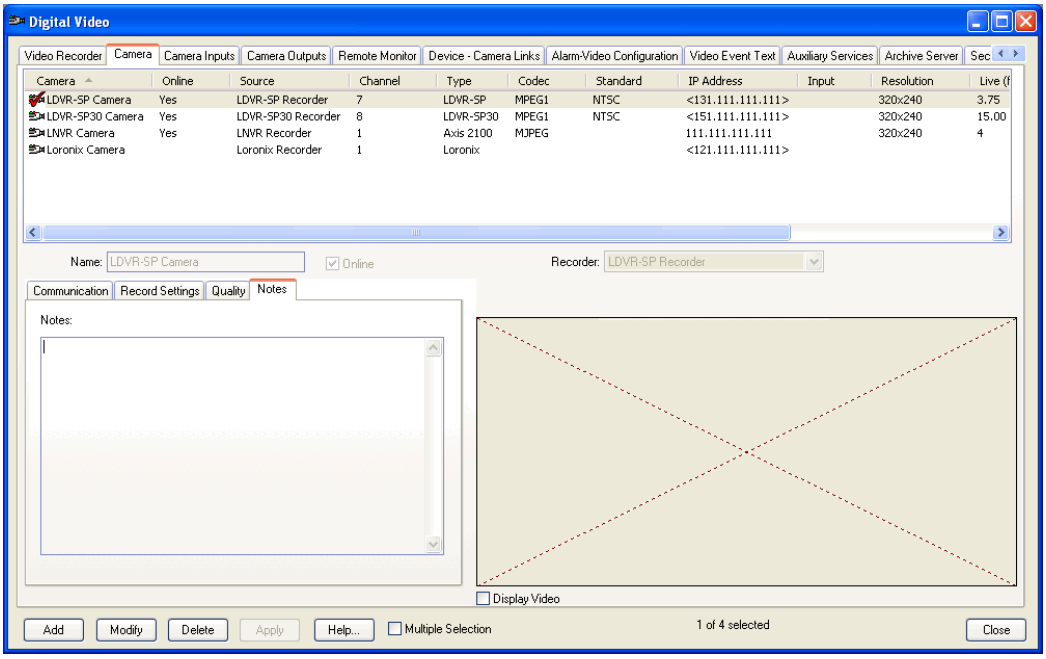
RTSP Port

This port is the TCP/IP port for RTSP protocol that provides session setup and control. By default, the RTSP port is 554 as defined by Internet standards. This field is available for use in the case that the port has been changed on the camera, or if the camera provides RTSP protocol on a different port. If changing the port, enter 554 or a value between 1024 and 65535.

Reset to Defaults

Click this button to return the RTP settings to the default values.

Camera Form (Notes Sub-tab)



Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

Camera Form Procedures

Use the following procedures on this form.

Configure LNVR Cameras

Note: Before you configure an LVNR camera, you must configure the LNVR recorder. For more information, refer to Add LNVR Video Recorders on page 933.

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click the Camera tab.
3. Click [Add].
4. In the **Name** field, enter a unique, descriptive name for the camera.
5. Select the **Online** check box to place the camera online.
6. From the **Recorder** drop-down, select the recorder that this camera communicates with.
7. Select the failover recorder. For more information, refer to Add LNVR Failover Video Recorders on page 934.
8. On the Connection sub-tab:
   a. Select the camera type from the drop-down.
   b. Some camera types require you to select a video standard (NTSC or PAL).
   c. Enter an IP address and port. The camera itself must have the same IP address as what you enter in this field.
   d. Once you enter the camera’s IP address, you can click [Camera Web Page] to open the selected camera’s configuration Web page.
   e. If the camera is configured to require authentication, then enter the valid username/ password. Otherwise, leave these fields blank.
9. Select the **Display Video** check box to preview the camera image.
10. On the Video sub-tab:
    a. Select an image resolution (number of pixels across and down).
    b. Select the degrees of rotation. If your camera is a ceiling mount the degrees of rotation should be “0”; desk mounted cameras should be “180”.
    c. Select the **Monochrome** check box if you want video recorded in black and white. This check box displays for specific camera types.
    d. Enter the default playback pre-roll and playback post-roll. Refer to the Camera Form (Video Sub-tab) on page 947 for field definitions.
    e. Enter the compression.
    f. Enter how much physical space (bits not bytes) one second of audio or video requires. Select the **Auto** check box if you want to accept the default (auto) settings.
11. On the Video Sensor sub-tab, enter the image settings for the camera. Refer to Camera Form (Video Sensor Sub-tab) on page 949 for field definitions.

12. On the Audio sub-tab:
    a. Select a source type from the drop-down.
    b. Adjust the volume using the slider.
13. On the Normal Mode sub-tab:
    a. Select the frame rate to display live video in Alarm Monitoring.
    b. Specify when video recording should occur by selecting the **Recording Timezone** from the drop-down.
    c. Do one of the following:
        - Select the **Continuous Recording** check box if you want video recorded at a constant frame rate. Enter the frames per second.
        - Select the **Time-Lapse Recording** check box if you want a slower frame rate when no motion is detected. Enter the seconds per frame.

    Note: The frame rates during an event are configured on the Event Mode sub-tab. If event recording is configured, they will override any settings on the Normal Mode sub-tab when an event occurs.

    d. If you have configured archiving for the LNVR, you may specify a timezone to **Archive Continuous Video** from the drop-down. For more information, refer to Archive Server Form on page 988.
    e. Select the **Audio** check box if you wish to enable audio.
        - Select the **Recording** check box if you wish to record audio.

    Notes: Audio is only recorded when video is also recording.

    With the In-Camera Storage feature it is not necessary to select the **Recording** check box. Recorded video will automatically include audio when the **Audio** check box is selected.

    f. Select **Use Camera Time Stamps** to obtain time stamps from the camera.
14. On the Event Mode sub-tab, select the **Event Recording** check box if you want to increase frame rates per second before and during an event. When the event ends, non-event recording mode resumes. Refer to Increase Frame Rates During Events on page 966 for additional information.
15. Click [OK].

Configure LDVR, Generic Video, or Loronix Cameras

Note: Before you configure a camera, you must configure the recorder. For more information, refer to Add LDVR, Generic Video, or Loronix Video Recorders on page 935.

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click the Camera tab.
3. Click [Add].
4. In the **Name** field, enter a unique, descriptive name for the camera.
5. From the **Recorder** drop-down, select the recorder that this camera communicates with.

Note: Generic Video, LDVR-SP, LDVR-SP30, LDVR-408, LDVR-444, and Loronix recorders support any analog camera.

6. On the Communications sub-tab, do one of the following:

- For cameras with a LDVR-SP, LDVR-SP30, LDVR-408, or LDVR-444 recorder:
  i. Enter the channel number that the camera connects to. Each camera must be on its own unique channel.
  ii. If you want the selected camera to generate an alarm when motion is detected, select the timezone from the **Generate Motion Detection** drop-down. Click [Motion Detection Configuration] to set the level of motion sensitivity. For more information, refer to Configure Motion Detection and Apply Motion Mask to a Camera on page 967.
  iii. For cameras with LDVR-SP, LDVR-SP30, LDVR-444 recorders, if you want the selected camera to generate an alarm when the image produced by the camera has the same color throughout the entire image (typically all black or all white), select the timezone from the **Generate Blind Camera Alarms** drop-down.
  iv. For LDVR-SP recorders, select a time zone from the **Archive Continuous Video** drop-down if you want continuous archiving to be turned on for this camera. The video recorder must also be configured for continuous archiving.
  v. If the selected camera is connected to a matrix switcher, choose the switcher from the **PTZ Controlled by Matrix Switcher** drop-down. In the **Matrix Channel** field, enter the matrix input channel number the camera connects to. If the camera is linked to a virtual matrix switcher, enter the drop-in address instead of a channel number. This address needs to match the one set on the camera via a dip switch.
- For cameras with a Generic Video or Loronix recorder:
  i. In the **Camera ID** field, enter a unique ID number for the camera.
  ii. Select the **Display Motion Detection Alarms** check box if you want an alarm to be displayed in Alarm Monitoring when this camera detects motion.
  iii. If the selected camera is connected to a matrix switcher, choose the switcher from the **PTZ Controlled by Matrix Switcher** drop-down.
  iv. In the **Matrix Channel** field, enter the matrix input channel number the camera connects to.

7. On the Record Settings sub-tab do one of the following:
   - For cameras with a Generic Video or Loronix recorder enter the default pre-roll and post roll of an event. Refer to the Camera Form (Record Settings Sub-tab) on page 944 for field definitions.
   - For cameras with an LDVR-SP, LDVR-SP30, LDVR-408, LDVR-444 video recorder:
     i. Select the frame rate to record video.
     ii. Enter the compression.
     iii. Select the **Enable Audio Recording** check box if you want to enable audio recording for live and recorded video for the selected camera. Audio recording can be enabled for each camera per recorder.
     iv. Enter the default pre-roll and post-roll of an event. Refer to the Camera Form (Record Settings Sub-tab) on page 944 for field definitions.
8. Select the **Display Video** check box to preview the camera image.
9. On the Quality sub-tab do one of the following:
   - For cameras with a Generic Video or Loronix recorder, skip this step and proceed to the next numeric step.
   - For cameras with any other video recorder, enter image quality settings for the camera. Refer to Camera Form (Quality Sub-tab) on page 946 for field definitions.
10. Click [OK].

Add or Delete NetDVMS or goVision Cameras

NetDVMS and goVision cameras cannot be manually added or deleted in OnGuard. To add or delete cameras, perform the operation on the video recorder and then import the configuration from the Video Recorder form in System Administration.

Capture Video on Event Only

Capture Video on Event Only is a feature designed for systems that have limited bandwidth. Devices can be configured to trigger the recording of events, thus eliminating the need for continuous video capture.

Note: When an event is generated, OnGuard sends a message to the LNVR to begin recording and the LNVR must establish connection with the camera. As a result, the first few seconds of the event may not be available. This loss can be minimized by reducing the load to the communication server, linkage server, LNVR, and by setting the camera at a higher frame rate.

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click the Camera tab.
3. Select a camera with an LNVR recorder.
4. Click [Modify].
5. Click the Normal Mode sub-tab.
6. Deselect the **Live** check box.
7. Click the Event Mode sub-tab.
8. Select the **Event Recording** check box.
   a. Select the **Frame Rate** from the drop-down.
   b. Enter the post-roll to record after the event occurs.

Note: You cannot set the Pre-Roll while live video capture is disabled.

9. Click [OK].
10. Configure one or more of the following to trigger the camera to enter event mode:
    - **Camera inputs**. Configure a camera input and select the **Trigger Camera Event Mode** check box. For more information, refer to Camera Inputs Form on page 969.
    - **Camera motion detection**. Configure camera motion detection on the Event Mode sub-tab by selecting a **Timezone** and the **Trigger Camera Event Mode** check box.
    - **Device-camera link and Alarm-video configuration**.

Notes: The Device-camera link and Alarm-video configuration will cause the camera to appear offline in Alarm Monitoring because there is not a continuous connection to the camera.

Devices can be used to trigger event mode by first setting up a Device-Camera link. For more information, refer to Add a Device - Camera Link on page 978.

Next use the Alarm-Video Configuration form to modify the alarm generated by the device. Select the **Begin Event Recording** radio button to trigger event mode on alarm. For more information, refer to Configure Video and Alarms on page 984.

Capture Video on Demand

Capture Video on Demand is a feature designed for systems with limited bandwidth. A connection is made to the camera only when video is requested by a user in the Alarm Monitoring application.

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click the Camera tab.
3. Select a camera with an LNVR recorder.
4. Click [Modify].
5. Click the Normal Mode sub-tab.
6. Select the live frame rate for the on demand video from the drop-down.
7. Deselect the **Live** check box.

Note: Capture Video on Demand will cause the camera to appear offline in Alarm Monitoring because there is not a continuous connection to the camera.

8. Click [OK].

Increase Frame Rates During Events

Cameras with LNVR recorders can be configured for event recording mode (increased frame rates during events with up to 5 seconds of pre-roll and post-roll time).

Note: This procedure only applies to cameras with LNVR recorders.

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click the Camera tab.
3. Select a camera with an LNVR recorder.
4. Click [Modify].
5. Click the Event Mode sub-tab.
6. Select the **Event Recording** check box.
7. Select the frame rate from the drop-down.

Note: If the selected frame rate is within the recommended range, the value will be displayed in green, otherwise it will be displayed in red.

8. Enter the pre-roll and post-roll.
9. Any alarm on the Alarm-Video Configuration form that has the **Begin Event Recording** radio button selected will use these event recording settings.

Estimate RAM Needed for Pre-roll

It is recommended to estimate the amount of RAM needed before setting pre-roll to a value higher than 30 seconds. If the system resources do not meet the estimated value, it is highly recommended to set a lower value. If the value is set too high, it may result in video storage failure or video overflow errors.

1. Select a camera on the Camera form.
2. On the Capacity sub-tab, press [Update].
3. From the table, use Recording Rate (Mbps) with the highest value. (Using the highest recording rate ensures that the amount of RAM is not underestimated.) The recording rate can also be obtained from the Storage Calculator.

4. Divide by 8 to convert to MB/s.
5. Multiply by the number of seconds for pre-roll value.
6. Multiply by the number of cameras with the same configuration, or repeat steps 3 through 5 for each additional camera and add to the total RAM.

   (Overall Recording Rate / 8) x PreRoll x Number Cameras = RAM (MB)

   For example: If the Overall recording rate for a camera was 0.8 Mbps, the desired pre-roll was 30, and there were a total of 10 cameras with that configuration: 0.8 Mbps / 8 * 30 sec pre-roll * 10 cameras = 30 MB RAM required.

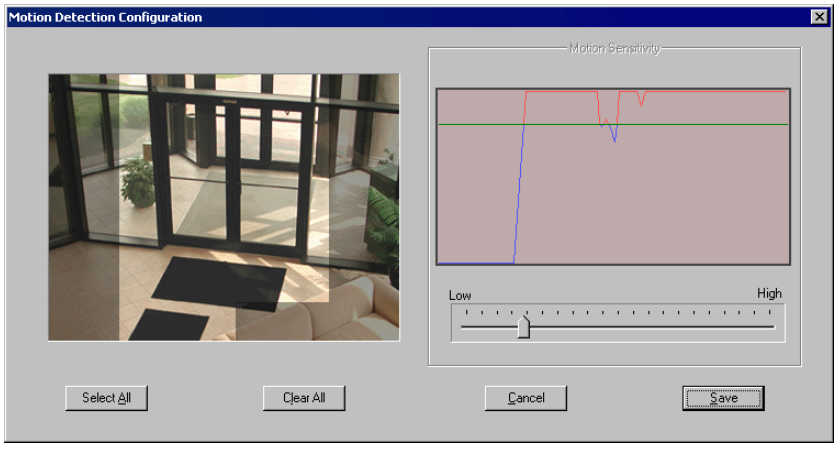
   (0.8 / 8) x 30 x 10 = 30
7. If the estimated RAM does not exceed the system resources available, configure the pre-roll according to your calculations. If the system does not have enough RAM to support the calculated configuration, adjust the length of pre-roll or number of cameras and re-calculate the RAM required.
8. Once pre-roll has been configured, monitor the CPU usage to determine whether system resource usage is acceptable.

Configure Motion Detection and Apply Motion Mask to a Camera

Notes: This procedure only applies to cameras with an LDVR-SP, LDVR-SP30, LDVR-408, or LDVR-444 recorder. To configure motion detection for cameras with an LNVR, refer to the Video Processing Form on page 998.

Cameras and recorders must be previously configured before completing this procedure. Otherwise, the Motion Detection Configuration button is disabled.

1. From the ***Video*** menu, select ***Digital Video***.
2. The Digital Video folder opens. Click the Camera tab.
3. Select the name of a camera.
4. Click the Communication sub-tab.
5. Click [Modify].
6. Click [Motion Detection Configuration]. The Motion Detection Configuration window opens.



7. Set the motion sensitivity to the desired level. The motion sensitivity level is how much motion the camera sees before it switches from a non-motion-detection state to a motion-detection state.

The camera will switch to a non-motion-detected state 10 seconds after the last time the amount of motion in front of the camera was at or above the motion sensitivity level.

Note: The red lines in the graph signify motion equal to or greater than the sensitivity level.

8. Select areas that will be masked for motion by clicking your cursor on the left side of the window. A gray box appears. To select several boxes, click and drag the mouse. To deselect boxes, right-click a box or right-click and drag the mouse.
9. Click [Save]. Motion will not be detected in masked areas.

Configure Time-Lapse Recording for LDVR Cameras

1. Enable time-lapse recording on the Video Recorder.
   a. On the Video Recorder form, select the video recorder from the listing window.
   b. Select the Recording sub-tab and click [Modify].
   c. Select the **Enable Time-Lapse Recording** check box.
   d. Set the **Non-Motion Frame Rate** in seconds per frame.
   e. Set the **Time Lapse Pre-Roll** to specify the amount of video to cache and record prior to an alarm.
   f. Click [OK].
2. Enable time-lapse recording for the individual camera.
   a. On the Camera form, select the camera from the listing window.
   b. Select the Record Settings sub-tab and click [Modify].
   c. Select the **Enable Time-Lapse Recording** check box.

Note: When the camera is in time-lapse mode, the value entered in the **Frame Rate** field must be 3.75 or higher if the recorder is configured for the NTSC (3.1 or higher for PAL).

3. To filter out unwanted motion, adjust the Motion Detection settings.
   a. Select the Communication sub-tab and click [Motion Detection Configuration].
   b. Set a mask for any areas with excessive motion by highlighting the area with the mouse.

Note: To mask all motion, click [Select All]. With this setting, the camera will never leave time-lapse mode.

   c. Adjust the slider to change the sensitivity threshold and eliminate false detections of motion.
   d. Click [Save] to retain the motion detection configuration changes.
4. Click [OK] to save the modifications to the camera settings.

Configure Time-Lapse Recording with Motion Detection for LNVR Cameras

Note: This configuration is just one example of how an LNVR camera can be configured to trigger time-lapse recording mode. For more information, refer to Time-Lapse Recording on page 920.

To configure time-lapse recording with the Motion Detection video event, complete the following steps:

1. Enable time-lapse recording for the individual camera.
   a. On the Camera form, select the camera from the listing window.

b. Select the Normal Mode sub-tab and click [Modify].
c. Select the **Time-Lapse Recording** check box.
d. Set the **Seconds per frame** value for the time-lapse recording rate.
e. Click [OK] to save the modifications to the camera settings.

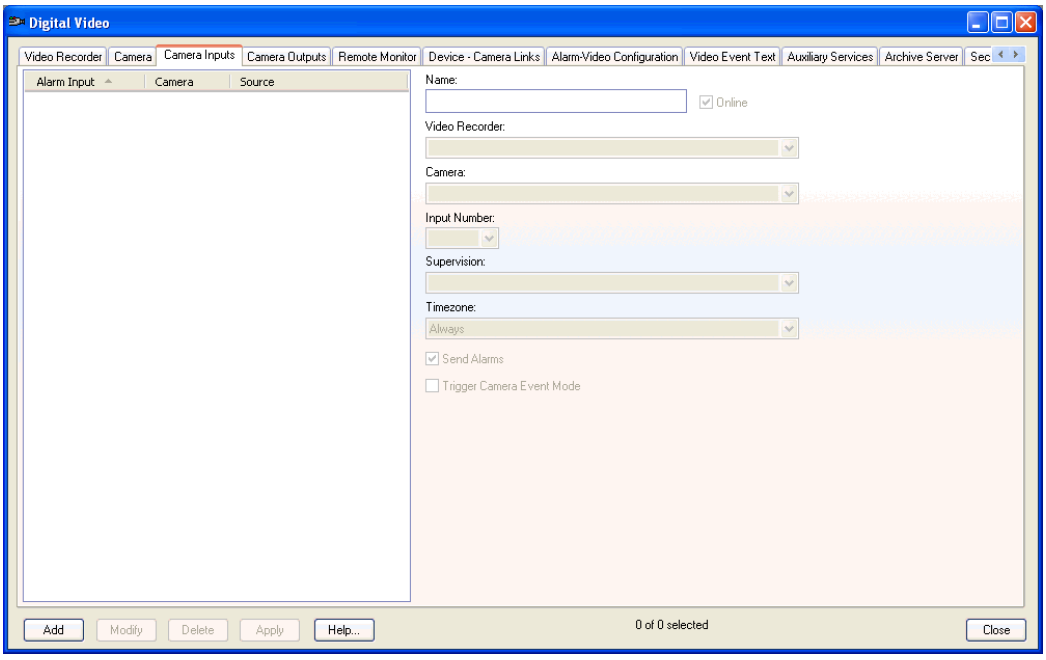
2. To trigger normal recording mode when motion is detected, create a Video Processing event.
   a. On the Video Processing form, add a Motion Detection (AI) event. For more information, refer to Add Event Settings on page 1006.
   b. Launch the Event Configuration/Search dialog by clicking the button.
   c. Set the **Region Of Interest** for the area you wish to monitor for motion.
   d. Adjust the **Threshold** if needed to eliminate false motion detection.
   e. Click [OK] to save the configuration.
   f. Click [OK] to save the Video Processing event.

Enter Notes for a Camera

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Camera Inputs Form

Camera inputs allow the configuration, monitoring, and linkage of alarms to other devices. The LNVR monitors the inputs and sends the alarms to Alarm Monitoring. Refer to the camera manufacturer documentation for connection information.



Name
A descriptive name for the camera input. This is a “friendly” name assigned to each camera input to make it easy to identify. Each name must be unique and contain no more than 32 characters.

Online
Select this check box to set the camera input online.

Video Recorder
Select the LNVR for the camera from the drop-down.

Camera
Select the camera for this input device.

Input Number
Enter the pin number for the input device.

Supervision
Select the normally open/closed setting from the drop-down. Refer to the camera/encoder documentation for additional information on selecting the correct normally open/closed setting.

Timezone
Select the access control timezone for monitoring the camera input.

Send Alarms
Select this check box to enable the sending of alarms generated by the camera input to Alarm Monitoring.

Trigger Camera Event Mode
Select this check box to force the camera to go to event mode recording upon a change on the input.

Add
Create a new camera input.

Modify
Enables changes to be made to the selected camera input.

Delete
Removes the selected camera input.

Help
Displays online help for this topic.

Close
Closes the Digital Video folder.

Camera Inputs Form Procedures

Use the following procedures on this form.

Add a Camera Input

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Camera Inputs tab.
3. Click [Add].
4. In the **Name** field, enter a unique, descriptive name for the camera input.
5. Select the **Online** check box to place the input online.
6. From the **Video Recorder** drop-down, select the recorder that this camera communicates with.
7. From the **Camera** drop-down, select the camera for this input.
8. Enter the number of the input device.
9. From the **Supervision** drop-down, specify whether the input is Normally Open or Normally Closed.
10. Select the access control timezone during which the input will be monitored.
11. Select the **Send Alarms** check box if you want to have alarms sent to Alarm Monitoring.
12. Select the **Trigger Camera Event Mode** check box if you want to force the camera into event mode recording upon a change in the input.
13. Click [OK].

Modify a Camera Input

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Camera Inputs tab.
3. In the listing window, select the camera input you want to change.
4. Click [Modify].
5. Make any changes you want to the camera input. You cannot change the video recorder, camera, or input number settings.
6. Click [OK].

Delete a Camera Input

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Camera Inputs tab.
3. In the listing window, select the camera input you want to remove.
4. Click [Delete].
5. Click [OK].

Add a goVision Camera Input

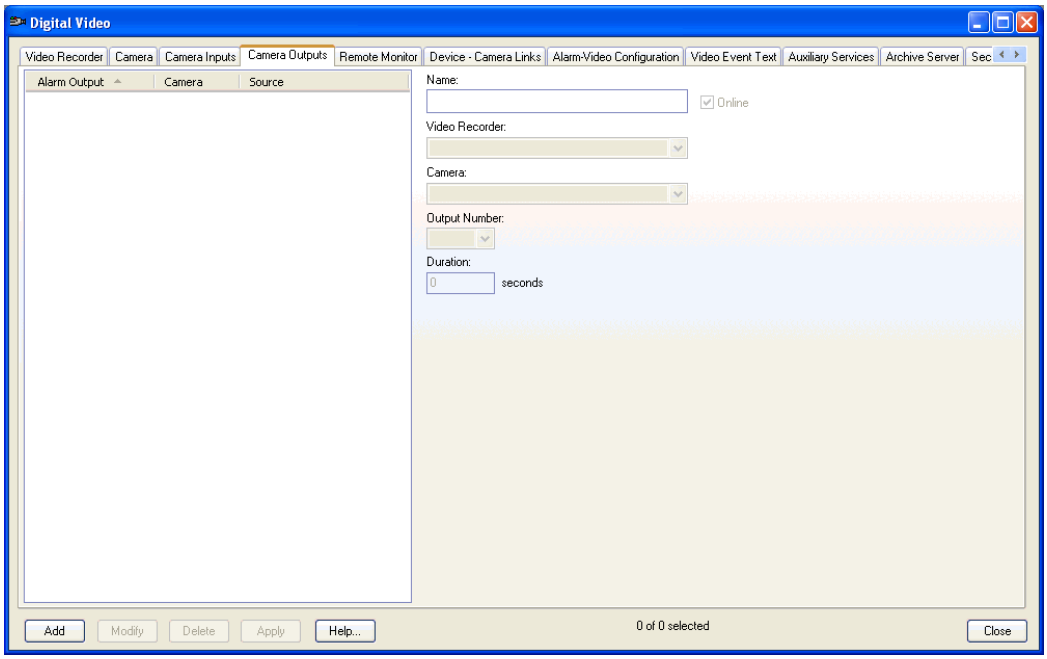
Camera inputs for goVision recorders are configured similarly to alarm panels.

1. From the ***Access Control*** menu in System Administration, select ***Alarm Panels***.
2. In the **Alarm Panel Name** field, type a unique, descriptive name for the alarm panel.
3. Select the goVision recorder from the **Panel** drop-down.
4. Select “Recorder Dry Contacts” from the **Type** drop-down.
5. Click [OK].
6. Click the Alarm Inputs tab.
7. Select the name of the goVision alarm panel from the listing window.

8. Click [Add].
9. In the **Name** field, type a unique, descriptive name for the input.
10. Select a **Supervision** from the drop-down.
11. Specify the **Input Number**.
12. Click [OK].

Camera Outputs Form

Camera outputs allow the configuration and linkage of alarms to other devices. Camera outputs can be placed in Output Device Groups and selected as devices on the output side of a Global I/O linkage. Refer to the camera manufacturer documentation for connection information.



Name

A descriptive name for the camera output. This is a “friendly” name assigned to each camera output to make it easy to identify. Each name must be unique and contain no more than 32 characters.

Online

Select this check box to set the camera output online.

Video Recorder

Select the LNVR for the camera from the drop-down.

Camera

Select the camera for this output device.

Output Number

Enter the pin number for the output.

Duration
Enter the pulse time for the output.

Add
Create a new camera output.

Modify
Enables changes to be made to the selected camera output.

Delete
Removes the selected camera output.

Help
Displays online help for this topic.

Close
Closes the Digital Video folder.

Camera Outputs Form Procedures

Use the following procedures on this form.

Add a Camera Output

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Camera Outputs tab.
3. Click [Add].
4. In the **Name** field, enter a unique, descriptive name for the camera output.
5. Select the **Online** check box to place the output online.
6. From the **Video Recorder** drop-down, select the recorder that this camera communicates with.
7. From the **Camera** drop-down, select the camera for this output.
8. Enter the number of the output device.
9. For the **Duration** field, enter the pulse time for the output.
10. Click [OK].

Modify a Camera Output

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Camera Output tab.
3. In the listing window, select the camera output you want to change.
4. Click [Modify].
5. Make any changes you want to the camera output. You cannot change the video recorder, camera, or output number settings.
6. Click [OK].

Delete a Camera Output

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Camera Outputs tab.
3. In the listing window, select the camera output you want to remove.
4. Click [Delete].
5. Click [OK].

Add a goVision Camera Output

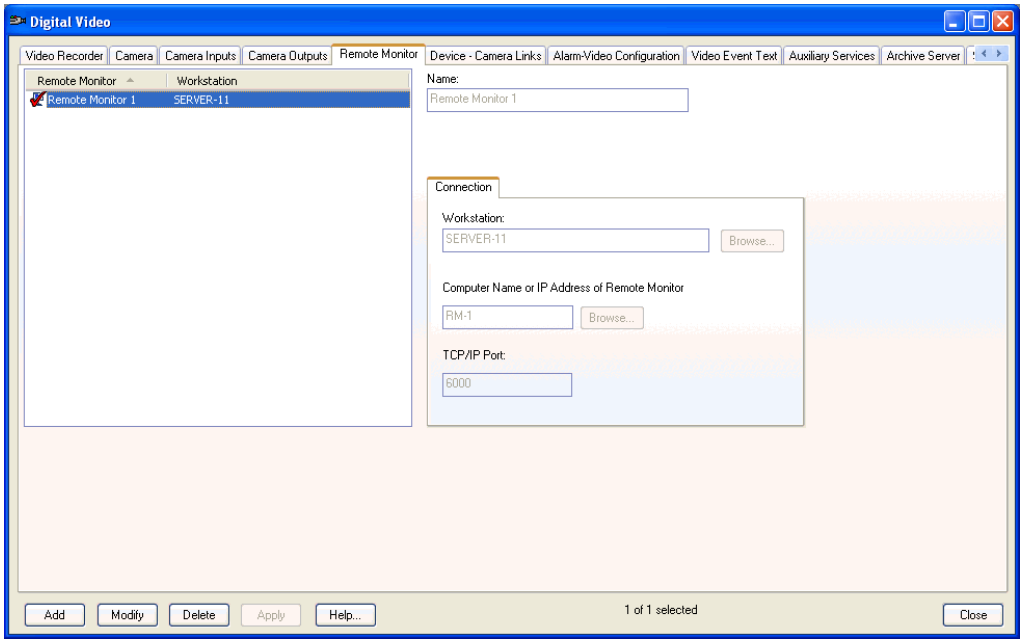
Camera outputs for goVision recorders are configured similarly to alarm panels.

1. From the ***Access Control*** menu in System Administration, select ***Alarm Panels***.
2. In the **Alarm Panel Name** field, type a unique, descriptive name for the alarm panel.
3. Select the goVision recorder from the **Panel** drop-down.
4. Select “Recorder Output Panel” from the **Type** drop-down.
5. Click [OK].
6. Click the Alarm Outputs tab.
7. Select the name of the goVision alarm panel from the listing window.
8. Click [Add].
9. In the **Name** field, type a unique, descriptive name for the input.
10. Specify the duration and the output number for the output.
11. Click [OK].

Remote Monitor

Remote Monitor (RM), also commonly referred to as “camera call-up”, is an application that can be run on any PC without OnGuard installed. The RM is installed on a client from the Supplemental Materials disc and configured in System Administration. The RM application behaves as a slave to the Alarm Monitoring application which is used to send video commands.

Special considerations must be made for RM clients connecting an LNVR with security settings configured. For more information, refer to LNVR Security on page 976.



Name
A descriptive name for the Remote Monitor.

Workstation
Enter the name or IP address of the workstation that runs the Communication Server.

Browse
Click this button to browse for the workstation or RM computer name.

Computer Name or IP Address of Remote Monitor
Enter the computer name or IP address of the computer that the RM runs on.

TCP/IP Port
Enter the connection port for the Remote Monitor. The same port number must also be configured in the Remote Monitor application. For more information, refer to the Alarm Monitoring User Guide.

Add
Create a new Remote Monitor entry.

Modify
Enables changes to be made to the selected Remote Monitor.

Delete
Removes the selected Remote Monitor.

Help
Displays online help for this form.

Close
Closes the Digital Video folder.

LNVR Security

Currently there is no secure communication between the RM and the OnGuard software. The RM must use another method of authentication to an LNVR with security settings because it cannot receive credentials from the OnGuard server. To enable authentication with the LNVR, log on to the RM client with a Windows user account that belongs to the LNVUsers group or configure RM to run as a LNVUsers group member.

Notes: If anonymous DCOM is disabled on the LNVR, the Windows user logged on to the RM client must be authenticated by the LNVR as Everyone or Administrator.

goVision recorders must have their username and password set to the default values to view video in Remote Monitor.

NetDVMS recorders must have their username set to “sp911” and password set to “lenel” to view video in Remote Monitor.

Remote Monitor Form Procedures

Use the following procedures on this form.

Add a Remote Monitor

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Remote Monitor tab.
3. Click [Add].
4. In the **Name** field, enter a unique, descriptive name for the remote monitor.
5. In the **Workstation** field, enter the name or IP address of the workstation running the Communication Server, or click [Browse] to search for it.
6. In the **Computer Name or IP Address of Remote Monitor** field, enter the name or IP address of the remote monitor, or click [Browse] to search for it.
7. In the **TCP/IP Port** field, enter the communications port of the remote monitor.
8. Click [OK].
9. The Monitor Zone Assignments window is displayed. Select the monitor zone(s) you wish to assign the remote monitor to and click [OK].

Modify a Remote Monitor

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Remote Monitor tab.
3. In the listing window, select the remote monitor you wish to change.
4. Make the changes you want to the remote monitor.
5. Click [OK].

Delete a Remote Monitor

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Remote Monitor tab.
3. In the listing window, select the remote monitor you wish to delete.

4. Click [Delete].
5. Click [OK].

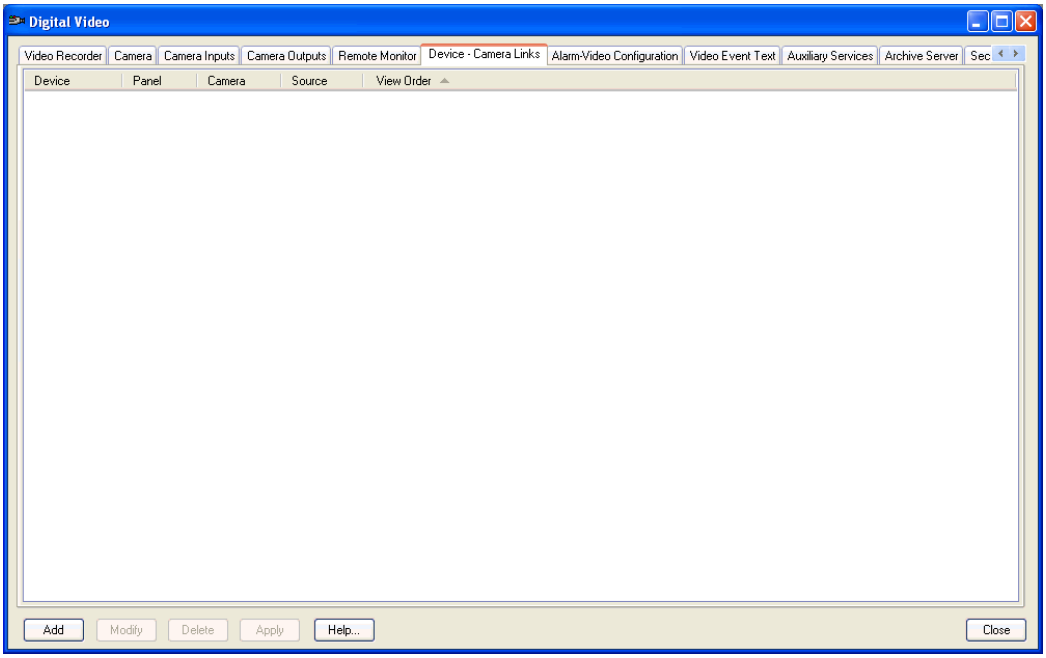
Device - Camera Links Form

Devices can be configured to trigger a camera response when alarms are generated by the device. The Device-Camera Links form defines the relationship between the camera and the device. The Alarm-Video Configuration form can then be used to specify the action performed by the camera when an alarm is generated by the device.

Camera to camera links can also be created with the Device - Camera Links form. When viewing video for an alarm with associated video, video for any linked cameras will also be launched with the parent camera. If you also want to view video for the associated cameras when launching the parent camera from the System Status Tree, add the following line to the `[DigitalVideo]` section of the **ACS.INI** file: `AlwaysIncludeCameraToCameraLinks=1`

> **IMPORTANT:** Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

Device-camera links for goVision cameras require additional configuration on the recorder. For more information, refer to Add a Device - Camera Link for a goVision Camera on page 979.



Listing window

Lists currently defined device-camera links.

Add

Launches the device-camera link wizard.

Modify

Enables changes to be made to the selected device-camera link.

Delete
Removes the selected device-camera link.

Help
Displays online help for this topic.

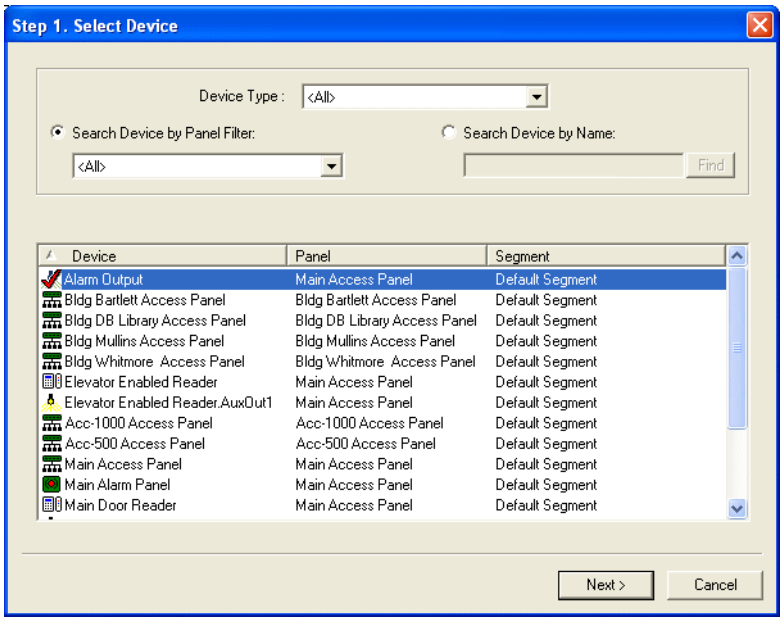
Close
Closes the Digital Video folder.

Device - Camera Links Form Procedures

Use the following procedures on this form.

Add a Device - Camera Link

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Device-Camera Links tab.
3. Click [Add]. The Select Device window opens.



4. Do one of the following:
   - Select the **Search Device by Panel Filter** radio button, and then select a device type and a panel filter from the drop-downs. The names of the devices that match your search will be displayed in the listing window.
   - Select the **Search Device by Name** radio button if you know the name of the device you want to link. Type in the name of the device, and then click [Find]. If the name you entered is located in the system, it will be displayed in the device listing window.
5. In the listing window, click on the name of the device you want to link. A red checkmark will appear next to the name of the selected device.
6. Click [Next]. The Select camera(s) window opens.

7. Select a recorder from the **Video Recorder** drop-down. The names of the corresponding cameras will be displayed in the listing window.
8. In the cameras listing window, select the name of the camera(s) that you want to link. The names of selected cameras will appear in the linked cameras listing window.

Note: Clicking on an already selected camera in the cameras listing window will remove that camera from the linked cameras listing window.

9. Click the **View order** spin buttons to set the priority of the selected camera in the linked cameras listing window.
10. Click [Save Link(s)]. The Summary window opens.
11. Click [Finish] to complete the wizard, or [Add More] to return to the Select Device window where you can add more device-camera links.

Note: If you are adding a device-camera link to a reader input or alarm panel input, you must also create a link to the parent device for the link to function properly.

Add a Device - Camera Link for a goVision Camera

1. Configure the goVision DVR recording to either “Alarm,” “Motion or Alarm,” or “Continuous or Event”.
2. Configure the goVision DVR inputs such that input 1 is linked to camera 1, input 2 is linked to camera 2, etc.
3. Set the schedule for the input. When an alarm occurs for the device linked to camera 1 it will trigger input 1 to start event recording.
4. Complete the steps to configure the device-camera link in OnGuard. For more information, refer to Add a Device - Camera Link on page 978..

Modify a Device - Camera Link

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Device-Camera Links tab.
3. In the listing window, select the device-camera link you wish to change.
4. Click [Modify] to launch the device-camera link wizard. The Select camera(s) window opens.
5. Make the changes you want to the link.
6. Click [Save Link(s)]. The Summary window opens.
7. Click [Finish] to complete the change, or [Add More] to return to the Select camera(s) window where you can modify other device-camera links.

Delete a Device - Camera Link

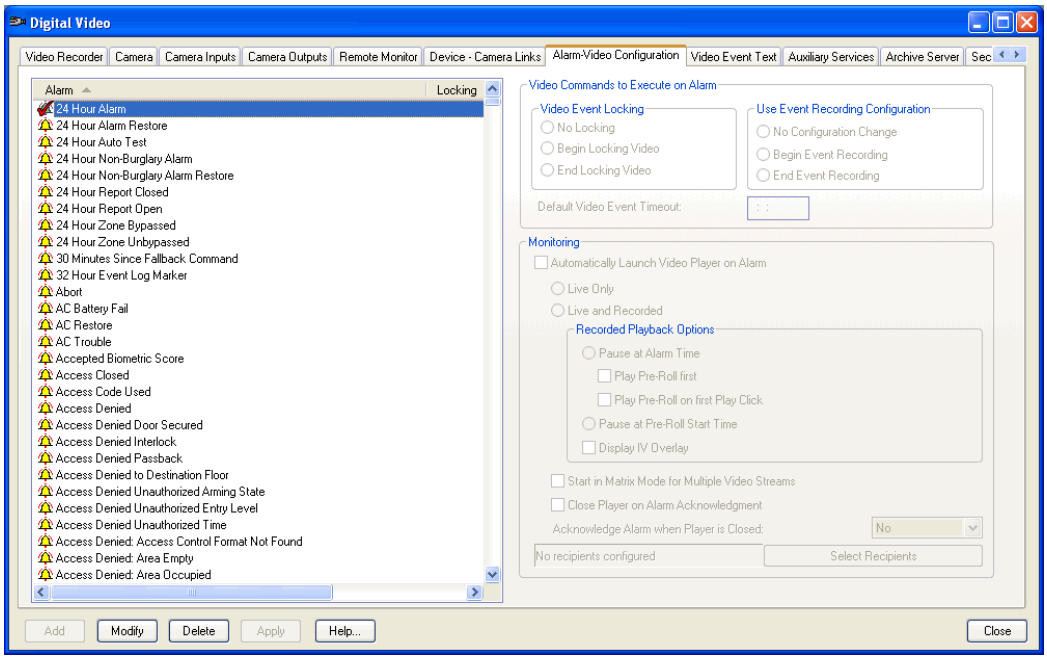
1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Device-Camera Links tab.
3. In the listing window, select the device-camera link you wish to delete.
4. Click [Delete].
5. Click [OK].

Alarm-Video Configuration Form

This form is used to configure video commands to be executed when an alarm generated in the system. When an alarm is generated, it is sent to the Communication Server. The Communication Server sends the alarm to the Linkage Server. Based on your alarm-video configurations, the Linkage Server can then tell the video recorder to:

- Start locking a video clip or end locking a video clip
- Start event recording or end event recording
- Automatically launch video

Note: For alarm-video configurations to work properly, the Linkage Server must be configured and running.



Listing window

Lists currently defined alarms. The window contains all of the alarms that can have video commands associated with them.

No Locking

Select this radio button if you do not want video event locking when the selected alarm is generated.

Begin Locking Video

Select this radio button if you want the video recorder to start locking a video segment when the selected alarm is generated. When this option is selected, a default video event timeout must be set. This will ensure that the event ends and does not end up locking all of the video on the video recorder. If event locking is configured for primary LNVR recorders, then the corresponding secondary recorders will also lock video.

End Locking Video

Select this radio button if you want the video recorder to end the locking of a video event prior to the specified default video event timeout period when the selected alarm is generated. The system ignores this setting if the selected alarm is generated after the specified default timeout period.

No Configuration Change

Select this radio button if you do not want a event recording configuration change when the selected alarm is generated.

Begin Event Recording

Select this radio button if you want to switch to the specified event recording configurations (frame rate, resolution, compression, etc.) when the selected alarm is generated. When this option is selected, a default video event timeout must be set. This will ensure that the event recording configurations end and revert back to standing recording (or no recording), to avoid filling up the video recorder with unnecessary video.

End Event Recording

Select this radio button if you want the video recorder to end recording at the specified event recording configurations prior to the specified default video event timeout period when the selected alarm is generated. The system ignores this setting if the selected alarm is generated after the specified default timeout period.

Default Video Event Timeout

A value is required in this field if you selected the **Begin Locking Video** and/or **Begin Event Recording** radio buttons. Specify the timeout period in which to wait for another alarm to send the begin locking video or begin event recording command. If the timeout period expires before this happens, then the alarm will also send a end locking video, or end event recording command, thus completing the automatic video event creation process.

Automatically Launch Video Player on Alarm

If selected, Alarm Monitoring will automatically launch a video window displaying the alarming device's associated cameras. When a new video alarm occurs, an existing alarm window will be reused by default if one exists for that device. To open a new video window for each alarm, add the following line to the **ACS.INI** file in the `[DigitalVideo]` section on each workstation: `ReuseAlarmWindows=0`. Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

Live Only

Select this radio button to launch only live video on alarm.

Live and Recorded

Select this radio button to enable the Double Video on Alarm feature.

Pause at Alarm Time

Select this radio button to pause the recorded video at the time the alarm occurred.

Play Pre-Roll First

Select this check box to play pre-roll before pausing at the time of the alarm.

Play Pre-Roll on First Play Click

Select this check box to play the re-roll first when the play button is clicked.

Pause at Pre-Roll Start Time

Select this radio button to pause the recorded video at the beginning of the pre-roll.

Display IV Overlay

Select this check box to display the alarm overlay for IntelligentVideo alarms.

Start in Matrix Mode for Multiple Video Streams

Select this check box to launch video for multiple video streams in matrix mode.

This option must be used when Double Video on Alarm is enabled.

Close Player on Alarm Acknowledgment

Select this check box to have video windows closed as alarms are acknowledged.

Acknowledge Alarm when Player is Closed

Select one of the following options from the drop-down to specify the behavior for acknowledgement of alarms when the Video Player is closed:

- "No" - when the Video Player is closed the alarm will not be acknowledged
- "Yes" - when the Video Player is closed the alarm will automatically be acknowledged
- "Prompt" - when the Video Player is closed the user will be prompted to choose whether or not to acknowledge the alarm.

Select Recipients

Used to open the Assign Recipients dialog to select the recipients to push video to when the alarm is generated.

Add

This button is not used.

Modify

Enables changes to be made to alarm-video configurations.

Delete

Removes a video command from a selected alarm.

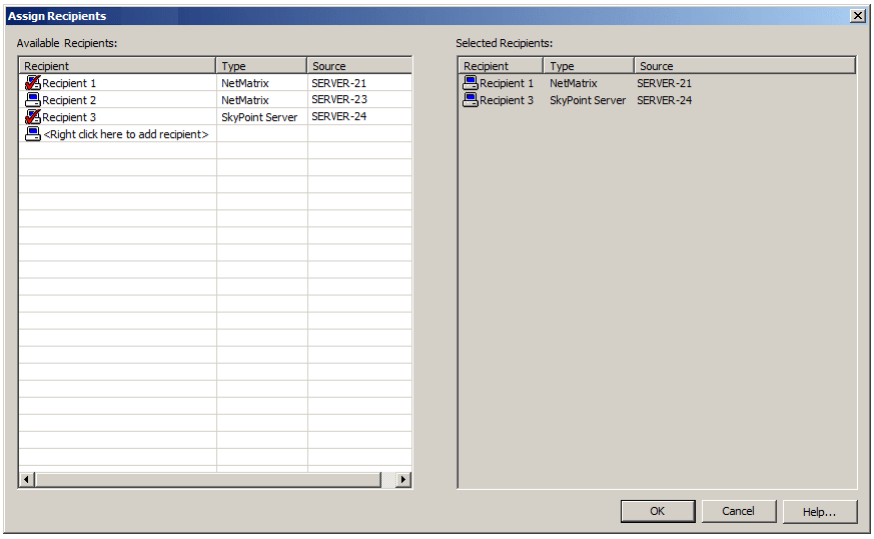
Help

Displays online help for this topic.

Close

Closes the Digital Video folder.

Assign Recipients Dialog



The Assign Recipients dialog is used to specify recipients for push video on alarm. Select (place a check mark beside) each recipient to send push video to when the alarm occurs.

This dialog supports three kinds of recipients: NetMatrix, external clients, and UserDefined. NetMatrix recipients are configured on the NetDVMS recorder and imported during the configuration import from the NetDVMS. external clients recipients are populated dynamically with all clients currently connected to the external client Server. UserDefined recipients can be added to specify an external clients recipient that is not currently online, but may be available when the alarm is generated.

Double Video on Alarm

If an alarm is configured to automatically launch the Video Player, you can configure it to launch recorded video in addition to live video. When this feature is enabled, recorded and live video are automatically launched matrix mode for each camera associated with the alarm.

It is highly recommended to set the playback pre-roll for the camera to at least 10 seconds when using this feature. For more information, refer to Camera Form (Connection Sub-tab) on page 942.

IMPORTANT: Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

To specify the maximum length of recorded video to load, add the following settings in the `[DigitalVideo]` section of the **ACS.INI** file.

```
AlarmDurationMax=60
```

Use this line to configure the length of the recorded video clip that will be launched. The default value is 60 seconds.

The size of the Video Player window will be automatically adjusted to display live and recorded video in pairs for up to 3 camera channels. Additional configuration may be necessary if more than 3 camera channels are linked in a video event to display the each camera channel as a pair of video cells (recorded and live).

By adding lines to the `[DigitalVideo]` section of the **ACS.INI** file of the local workstation, you can configure the layout of cameras in the matrix view. You can configure different displays that depend on the total number of video streams.

First, choose a base resolution for the window size calculations. This base resolution should keep the same ratio as the most commonly used resolution. For example, if the most commonly used resolution is 252x240, you can use a base resolution of 176x120 for determining the window size.

The number located after `DoublePlayerWidth` and `DoublePlayerHeight`, `<n>`, represents the number of video streams. The `DoublePlayerWidth<n>` and `DoublePlayerHeight<n>` values should then be set to a multiple of the resolution depending on the number of video streams you want to have in each row and column. For example:

To calculate the values needed to display 4 camera channels (8 video streams) with a resolution of 176x120 with two cameras (2 pairs of live and recorded video) on each of two rows, multiply the width by four video streams (176*4) and multiply the height by two rows (120*2). The following lines would need to be added to the **ACS.INI** file:

```
DoublePlayerWidth8=704
DoublePlayerHeight8=240
```

Alarm-Video Configuration Form Procedures

Use the following procedures on this form.

Configure Video and Alarms

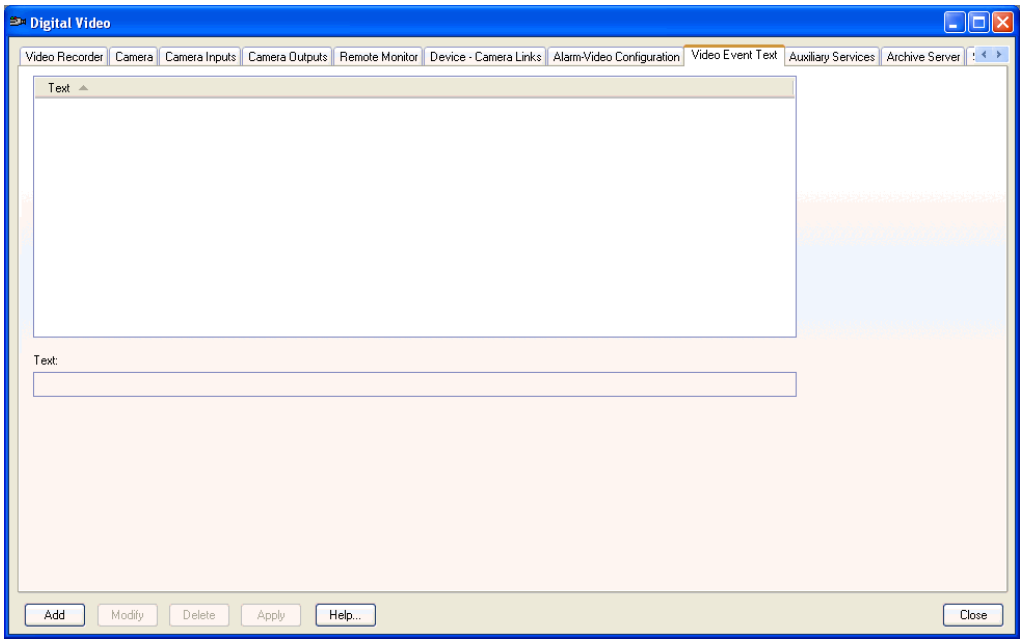
1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Alarm-Video Configuration tab.
3. Select an alarm from the listing window.
4. Click [Modify].
5. In the Video Event Locking section, do one of the following:
   - Select the **No Locking** radio button if you do not want video event locking when the selected alarm is generated.
   - Select the **Begin Locking Video** radio button if you want the video recorder to start locking a video segment when the selected alarm is generated. When this option is selected, a default video event timeout must be set. This will ensure that the event ends and does not end up locking all of the video on the video recorder.
   - Select the **End Locking Video** radio button if you want the video recorder to end the locking of a video event prior to the specified default video event timeout period when the selected alarm is generated. The system ignores this setting if the selected alarm is generated after the specified default timeout period.
6. In the Use Event Recording Configuration section, do one of the following:
   - Select the **No Configuration Change** radio button if you do not want a event recording configuration change when the selected alarm is generated.
   - Select the **Begin Event Recording** radio button if you want to switch to the specified event recording configurations (frame rate, resolution, compression, etc.) when the selected alarm is generated. When this option is selected, a default video event timeout must be set. This will ensure that the event recording configurations end and revert back to standing recording (or no recording), to avoid filling up the video recorder with unnecessary video.

- Select the **End Event Recording** radio button if you want the video recorder to end recording at the specified event recording configurations prior to the specified default video event timeout period when the selected alarm is generated. The system ignores this setting if the selected alarm is generated after the specified default timeout period.

7. If you selected the **Begin Locking Video** and/or **Begin Event Recording** radio buttons, in the **Default Video Event Timeout** field, specify the timeout period in which to wait for another alarm to send the begin locking video or begin event recording command. If the timeout period expires before this happens, then the alarm will also send a end locking video, or end event recording command, thus completing the automatic video event creation process.
8. Select the **Automatically Launch Video Player on Alarm** check box if you want Alarm Monitoring to automatically launch a view window displaying the alarming device's associated cameras.
9. Click [OK].
10. Verify that the Linkage Server is running.

Video Event Text Form

The Video Event Text form is used to enter text that can be used when a user manually creates a video event in Alarm Monitoring. Each entry on the Video Event Text form will appear in a drop-down for the user to select when manually generating a video event.



Listing window

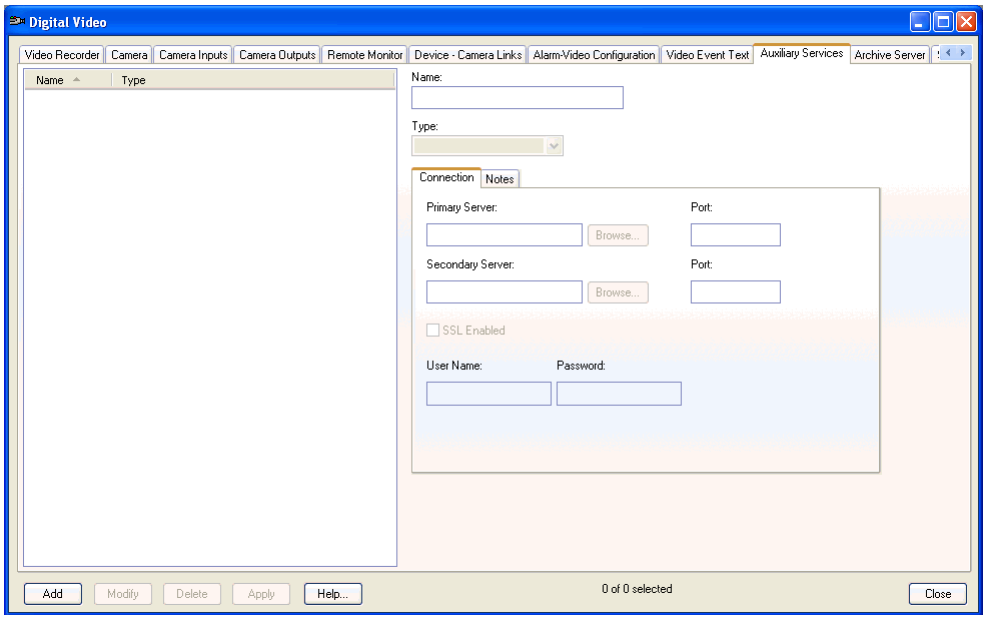
Displays currently available video event text.

Text

Enter the text that you wish to have available to a user when manually creating a video event.

Auxiliary Services Form

The Auxiliary Services tab is used to define servers that support Digital Video operations with external clients.



Auxiliary Services listing window

Lists currently defined Auxiliary Services. Video recorders are associated with an auxiliary services on the Auxiliary Services sub-tab of the Video Recorder form for a selected video recorder.

Name

A descriptive name for the auxiliary services.

Type

Select the type of auxiliary services from the drop-down.

Primary Server

Enter the name or IP address of the server that the primary server is running on. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Opens a Browse for Computer window, from which you can click on the name of a server.

Port

Set the **Port** field to 80.

Secondary Server

Enter the name or IP address of the server that the secondary server is running on. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse
Opens a Browse for Computer window, from which you can click on the name of a server.

Port
Set the **TCP/IP Port** field to 80.

SSl Enabled
Select if the servers are SSL enabled.

User Name and Password
Enter the user credentials for the auxiliary services. External clients must have a dedicated user account for this connection. This user should not be used to log in for any other function, as it will not appear in the external clients recipients lists.

Add
Create a new auxiliary services record.

Modify
Enables changes to be made to the selected auxiliary services record.

Delete
Removes the selected auxiliary services record.

Help
Displays online help for this topic.

Close
Closes the Digital Video folder.

Auxiliary Services Form Procedures

Use the following procedures on this form.

Add an External Client Server

Note: To communicate with OnGuard, port 7007 must be open on the external clients.

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Auxiliary Services tab.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this auxiliary services will be assigned to.
   b. Click [OK].
5. Select an external client from the **Type** drop-down.
6. Enter the location of the external clients in the **Computer Name or IP Address** text box, or click [Browse] to locate the server on the network.
7. In the **TCP/IP Port** field, enter “80”.

8. Enter the external clients user credentials in the **User Name** and **Password** fields. These credentials must be for a dedicated user account used only for this connection. This user should not be used to log in for any other function, as it will not appear in the external clients recipients lists.
9. Click [OK].

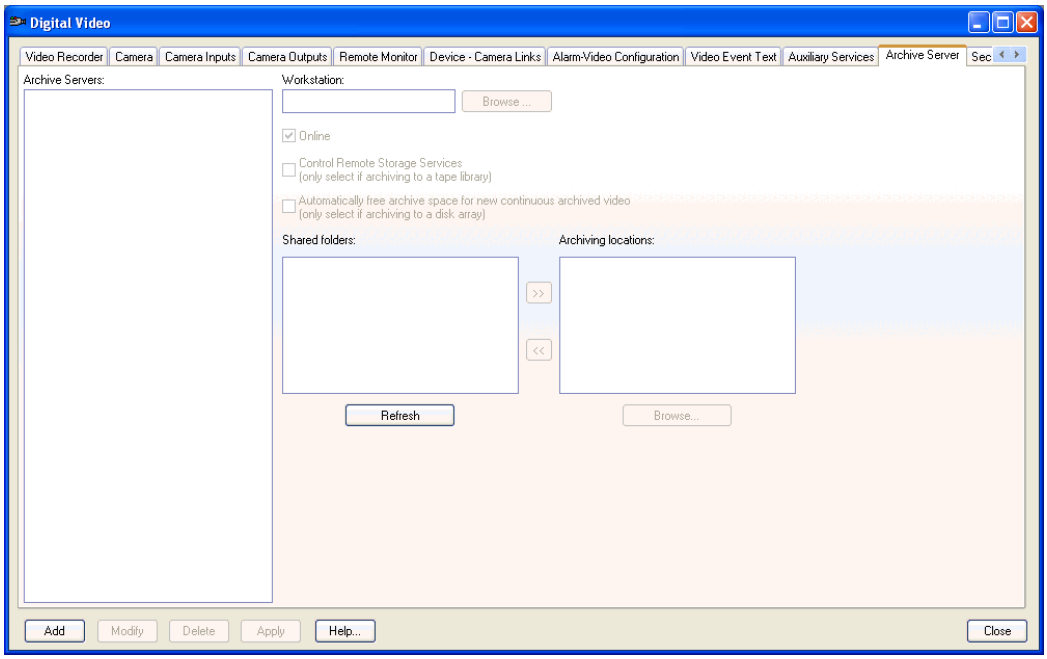
Configure Send Video with External Clients

Use this procedure to configure the Send Video feature on systems that have an external clients.

Note: With the external client's configuration it is not necessary to add the recpients to the NetDVMS. The external client recipient lists are populated automatically with the clients that are currently connected to the external clients.

1. Open port 7007 on the external client.
2. Perform a custom OnGuard installation to install the external clients component. For more information about custom installations, refer to the Installation Guide.
3. Add the external client on the Auxiliary Services tab in System Administration. For more information, refer to Add an External Client Server on page 987.
4. Link the NetDVMS to the external client on the Auxiliary Services sub-tab. For more information, refer to Video Recorder Form (Notes Sub-tab) on page 933.

Archive Server Form



Archive Servers listing window

Lists currently defined archive servers. For any archive server that has video recorders associated with it, the video recorders will be listed beneath the archive server. Video recorders are associated with an archive server by selecting the archive server in the **Archive Server** field on the Archiving/Purging sub-tab of the Video Recorder form for a selected video recorder.

Workstation

Select the name of the workstation that will be running the archive server. The archive server is responsible for communicating with the video recorder during archive operations. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Opens a Browse for Computer window, from which you can click on the name of a workstation.

Segment

Displays the segment that the archive server is a member of.

Online

If selected, the archive server will be online. Online indicates that the archive server is ready for use, that the Communication Server will attempt to communicate with it, and archiving will occur. If not selected, the Communication Server will not attempt to communicate with the archive server. This is useful when performing some maintenance tasks.

Control Remote Storage Services

This check box determines whether the archive server controls the Microsoft Remote Storage Services. The Services are used to move archived data to the tape library.

If selected, the archive server will activate the Microsoft Remote Storage Services when it fills the archiving locations. It will not archive any more data to the archiving locations until the Services move the data from the archiving locations to tapes, thereby creating more free space in the archiving location.

If not selected, when the archiving locations fill up, the administrator will have to manually move data from the archiving locations to tape to create more free space. Alternatively, you can choose to use the **Automatically free archive space for new continuous archived video** setting.

An archive server can use the **Control Remote Storage Services** setting or the **Automatically free archive space for continuous archived video setting**, but not both.

Automatically free archive space for new continuous archived video

This check box determines whether the archive server will delete the oldest archived video when there is no room for new archived video.This option is only for archiving to a disk array.

If selected, the archive server will delete the oldest archived continuous video blocks until there is enough free space to resume archiving.

If not selected, the archive server will never delete any archived continuous video. Instead, it will send an alarm to Alarm Monitoring saying that all archiving locations are full, and the administrator must free some space in the archiving location(s) before the archive server can resume archiving. As soon as the archive server detects that there is enough free space in the archiving location(s) to archive the next video blocks, it will automatically resume archiving.

Shared folders listing window

Lists all folders on the archive server workstation that are shared, but are not being used for archiving yet. If this field is blank and you have selected a **Workstation**, click [Refresh]. If the field is still blank, click [Browse] and select the shared folder you wish to use as an archiving location.

Right arrow

When clicked, moves a location that is selected in the **Shared folders** display to the **Archiving locations** display, effectively specifying it as an archiving location.

Left arrow

Enabled only in modify mode. When clicked, moves a location that is selected in the **Archiving locations** display to the **Shared folders** display, effectively removing it from the list of locations to archive to.

Refresh

Refreshes or reloads the list of shared folders. Click this button when you think shared folders on the archive server workstation have been changed or added.

Archiving locations listing window

Choose the locations where video will be put as it is archived. Each location should be in a UNC format such as **\\ArchiveServer\Directory** where the ArchiveServer is the name of the archive server you are configuring and Directory is the name of the directory to put the files in. Continuous archiving writes a new archive file to this directory every 5 minutes.

There is no limit to the number of archiving locations you can specify. The order in which the archiving locations are listed is not important because the archiving location with the most available space is always the location that will be written to first. When that location's drive fills, the system will automatically write archived files to the location in this list that has the largest amount of free space.

Browse

Opens a Browse for Folder window, from which you can click on a location of where the video events should be archived.

Selecting an archiving location using the [Browse] button is the functionally the same as selecting an archiving location in the **Shared folders** and using the right arrow button to move the location to the **Archiving locations**. Some networks may be configured in such a way that the **Shared folders** cannot be found. If this is the case, use the [Browse] button to locate the **Archiving locations**.

Add

Create a new archive server record.

Modify

Enables changes to be made to the selected archive server record.

Delete

Removes the selected archive server record.

Help

Displays online help for this topic.

Close

Closes the Digital Video folder.

Archive Server Form Procedures

Use the following procedures on this form.

Add an Archive Server

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Archive Server tab.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this archive server will be assigned to.
   b. Click [OK].
5. In the **Workstation** field enter the name of the workstation the archive server will be connected to.
6. If the archive server will be online, select the **Online** check box. Online indicates that the archive server is ready for use, that the Communication Server will attempt to communicate with it, and archiving will occur.
7. Select how the system will behave when the archiving locations run out of free space. Here are the options:
   - If the **Control Remote Storage Services** and **Automatically free archive space for new continuous archived video** check boxes are NOT selected, when the archive server fills the archiving locations, a message will be sent to Alarm Monitoring, and the administrator will have to make free space in the archiving locations.
   - If the **Control Remote Storage Services** check box is selected, the archive server will activate the Microsoft Remote Storage Services when it fills the archiving locations. It will not archive any more data to the archiving locations until the Services move the data from the archiving locations to tapes, thereby creating more free space in the archiving locations.
   - If the **Automatically free archive space for new continuous archived video** check box is selected, the archive server will delete the oldest archived continuous video blocks until there is enough free space to resume archiving.
8. Click [Refresh]. The shared folders on the specified workstation should be displayed in the Shared folders listing window.

Note: Some networks may be configured in such a way that shared folders will not display when the [Refresh] button is clicked. If this is the case, refer to the second procedure in step 9 to specify the archiving locations.

9. The system will write archived files in the order they are listed in the Archiving locations listing window. When the first location is full, the system will automatically write archived files to the second location, and so on. There is no limit to the number of archiving locations that can be specified. There are two ways a shared folder can be specified as an archiving location.
   a. The first way is:
      i. In the Shared folders listing window, click on the shared folder that you want to be an archiving location.
      ii. Click the right arrow button. The shared folder will be removed from the Shared folders listing window, and will be listed in the Archiving locations listing window.
      iii. Repeat steps i and ii for each shared folder that you wish to become an archiving location.
   b. The second way is:
      i. Click the [Browse] button that is below the Archiving locations listing window.
      ii. In the Browse for Folder window, navigate to the shared folder you wish to become an archiving location.

iii. Click [OK]. The location you selected will be listed in the Archiving locations listing window.

iv. Click [Refresh]. If the location you selected using the [Browse] button was listed in the Shared folders listing window, it will be removed.

v. Repeat steps i-iv for each shared location that you wish to become an archiving location.

10. Click [OK].

Modify an Archive Server

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Archive Server tab.
3. In the Archive servers listing window, select the archive server you wish to change.
4. Click [Modify].
5. Make any changes you want to the archive server. The workstation is the only setting that you cannot change.
6. Click [OK].

Delete an Archive Server

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Archive Server tab.
3. In the Archive servers listing window, select the archive server you want to remove.
4. Click [Delete].
5. Click [OK].

Security Form

LNVR video devices can be configured to require user authentication. If this occurs, valid user credentials (user name and password) must also be entered in the OnGuard system.

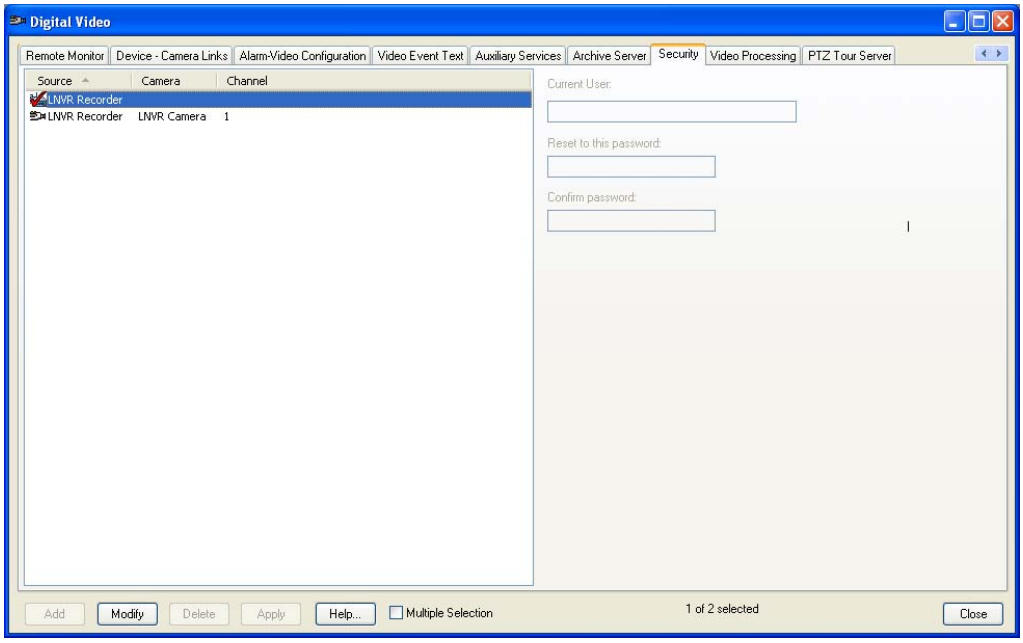
When you modify user credentials using a device specific configuration tool, you also need to make changes in the OnGuard system. For video recorders, the configuration tool would be a standard Windows administration tool. For cameras, the configuration tool would usually be the camera Web page, which can be launched from the Camera form.

A simpler method to change the password for the current user is via the Security form. There are two benefits to using this form. First, the task is completed in one step. OnGuard automatically communicates the new password to the device and updates the database. Second, you can modify passwords for more than one device at a time.

Notes: Password changes must conform to the password policies and standards configured by your system administrator.

goVision recorders must have their username and password set to the default values to view video in Remote Monitor and the VideoViewer browser-based client.

Before you modify the current user's password, OnGuard must be connected to the associated video device and the device must be online. The **Live** check box must be also selected in the Normal Mode sub-tab of the Camera folder. IP cameras must also be in secure mode. For more information, refer to IP Cameras on page 939.



Listing window

Lists currently defined LNVR recorders and cameras associated with them. Select the recorders and/or cameras you want to modify.

Current User

The name of the user account. This field automatically populates if a user name was initially populated on the Video Recorder/Camera forms and multiple devices are not selected in the Security form. If this field is blank, the password can not be changed.

Reset to this password

Enter the new password for the selected devices. The following restrictions apply:

- Axis cameras all up to 10 character passwords using A through Z, a through z, 0 - 9, !, #' - ', -, ., ^, _, ~, $
- Sony cameras allow up to 16 character passwords using A through Z, a through z, 0 - 9
- LNVR recorder password length is limited by the LNVR's computer password policy, which is set by the System Administrator. Valid characters are ! - ~

In addition to these restrictions, strong password rules apply if the strong password feature is enforced. For more information refer to chapter 1.

If the **Current User** field is blank, the password can not be changed.

Confirm password

Enter the new password a second time for verification.

Multiple Selection

Allows you to select more than one entry in the listing window.

Add

Does not apply to this form.

Modify

Enables changes to be made to the password for the selected devices.

Delete
Does not apply to this form.

Help
Displays online help for this topic.

Close
Closes the Digital Video folder.

Security Form Procedures

Use the following procedures on this form.

Change Network Video Password

LNVR passwords can be modified for previously configured LNVR video recorders and the cameras associated with them.

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Security tab.
3. Select one or several LNVR recorders and/or cameras. Use the **Multiple Selection** check box to select several entries.
4. Click [Modify].
5. Enter and confirm the new password.
6. Click [OK].

Notes: You can also modify previously configured passwords by:

Using the Change Network Video Password action type in the Scheduler folder. Devices do not have to be online when you configure the action. However, in order for action to succeed, the devices need to be online when the action is executed. For more information refer to the Scheduler folder.

or

Using the Global I/O folder to configure an output action to change the password. Devices do not have to be online when you configure the output action. However, in order for the output action to succeed, the devices need to be online when the input event occurs. For more information refer to the Global I/O folder.

Video Processing Form

For more information, refer to Video Processing Form on page 997.

PTZ Tour Server Form

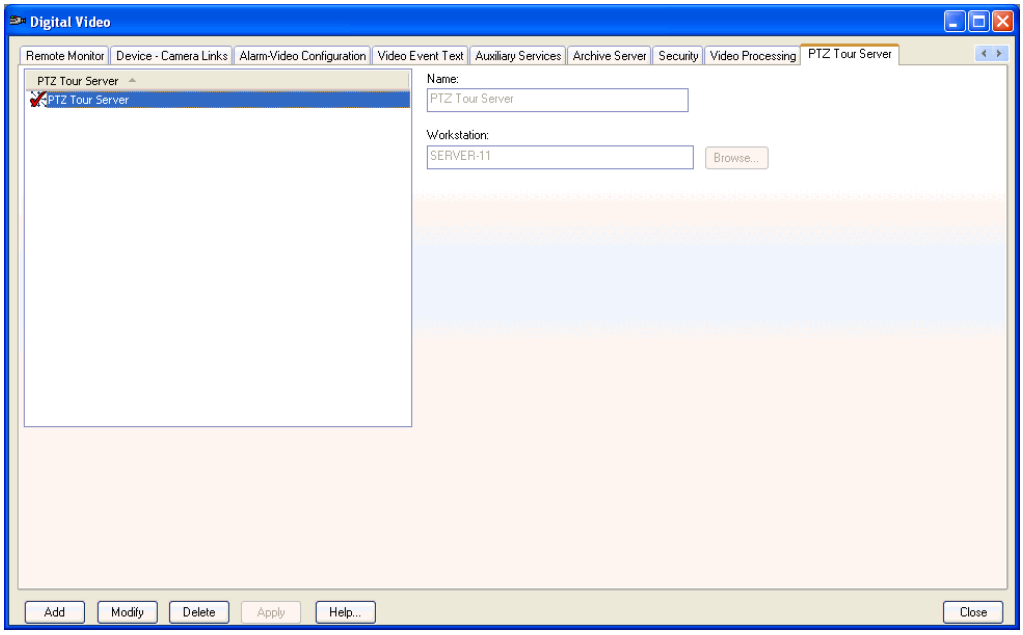
The PTZ Tour Server form is used to indicate a server running the PTZ Tour Server service. This service allows PTZ tours to run continuously in the background for recording purposes. PTZ tour

servers may be utilized by the Run PTZ Tour action type and when running a PTZ tour from Alarm Monitoring.

Background PTZ tours can only be interrupted by a user with a higher priority or by the user that started the tour. The PTZ timeout value is not utilized with background PTZ tours.

Notes: The PTZ Tour Server service can be run as a service in the background or as an application from the Windows Start menu.

The PTZ Tour Server service must be running on a workstation located in the same Region as the client using it.



Listing window

Lists currently defined PTZ tour servers.

Name

A descriptive name for the PTZ tour server.

Workstation

Select the name of the workstation that will be running the PTZ Tour Server service.

You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Opens a Browse for Computer window, from which you can click on the name of a workstation.

CHAPTER 48

Video Processing Form

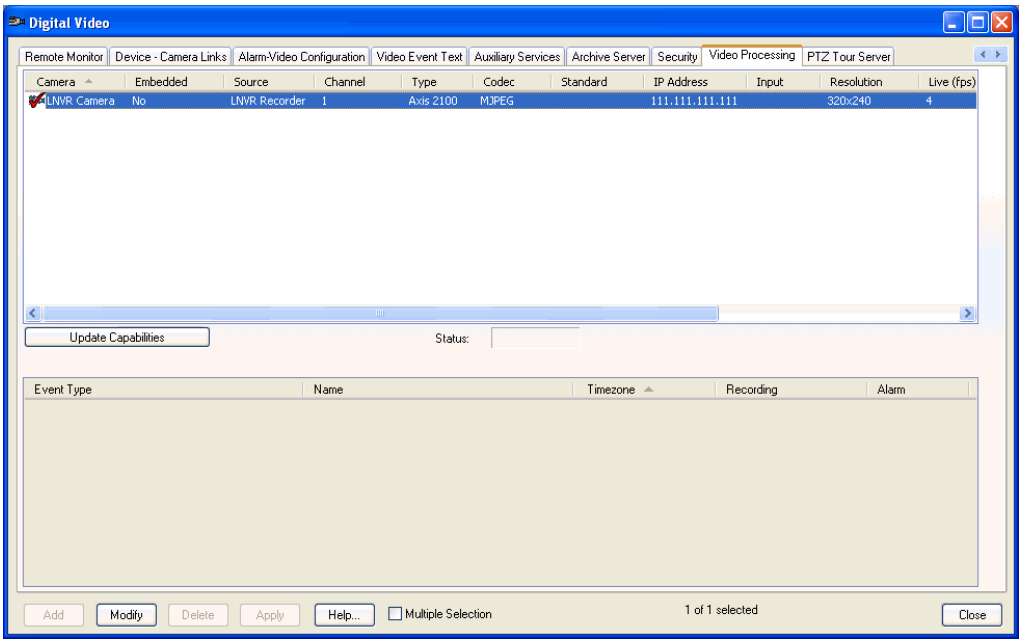
LNVR supports motion detection, blind camera, and brightness change events. OnGuard provides video configuration of these events through the Video Processing form. No additional licensing is required.

The Video Processing form is also used to configure the embedded IntelligentVideo events. These events are processed on the cameras rather than on the LNVR or IntelligentVideo Server.

To open the Video Processing form, select the ***Video*** **>** ***Digital Video*** menu item. Then select the Video Processing tab.

In addition to configuring multiple events for a specific camera, you can configure event properties on the Video Processing form. The Video Processing form includes a button that displays the Event Configuration/Search dialog where you can define event configuration parameters.

Video Processing Form



Listing window

Lists currently defined IP cameras on all LNVR recorders as well as the channel, camera type, video standard, camera IP address, camera resolution and frame rates. The Embedded column indicates the firmware version for embedded IntelligentVideo analytics if they are supported on the camera. The Embedded column indicates “No” if embedded analytics are not supported, or if the capabilities have not been updated for the camera. The [Update Capabilities] button is used to update the Embedded column.

Update Capabilities

Click this button to update the Embedded column to indicate whether embedded IntelligentVideo analytics are supported on the camera(s). Multiple cameras can be selected using the **Multiple Selection** check box.

Add Embedded Analytics Event

Click this button to launch the Embedded Analytics Configuration Wizard. For more information, refer to Add Embedded Analytics on page 1007.

Status

Displays the status of the selected recorder while configuring events in Modify mode.

Event Type

Displays the name of the configured event.

Name

A descriptive name for the event that will display in Alarm Monitoring. The name can be 21 characters long. Since OnGuard supports two events of the same type for the same camera, the name should be descriptive enough for Alarm Monitoring operators to recognize where the event occurred.

Timezone
The timezone during which the specified setting is active. Timezones are created in the Timezones folder, which is located by selecting ***Timezone*** from the ***Access Control*** menu.

Recording
The type of recording that will be used. Choices include:

- **Event** - increased frame rate with pre-roll for OnGuard specific events. Event recording settings are configured on the Event Mode sub-tab of the Camera form.
- **Normal** - continuous or time-lapsed recording. Normal recording settings are configured on the Normal Mode sub-tab of the Camera form.

Alarm
Determines whether an alarm displays in Alarm Monitoring.

- **On** - If the threshold is reached during the selected timezone, an alarm is sent from the recorder to OnGuard and an alarm displays in Alarm Monitoring.
- **Off** - If the threshold is reached during the selected timezone an alarm will not be active (sent to OnGuard) nor will it display in Alarm Monitoring.

Threshold
The level (percentage) that must be reached for an event to occur. This column displays only when the recorder is offline. When the recorder is online, the threshold value is configured on the Event Configuration/Search Dialog.

Displays the Event Configuration/Search dialog where you can configure event-specific parameters. For more information, refer to Event Configuration/Search Dialogs on page 1023.

Add
Does not apply to this form.

Modify
Enables changes to be made to the settings for the selected camera.

Delete
Deletes all configured events for the selected camera. Multiple cameras can be deleted by using the **Multiple Selection** check box.

Help
Displays online help for this topic.

Multiple Selection
Select this check box to select multiple entries in the listing window. This option only applies to the [Delete] and [Update Capabilities] buttons.

Close
Closes the Digital Video folder.

Video Processing Events

Video processing events are described as follows.

Blind Camera (AI)

Blind camera detection generates an alarm when the camera cannot capture the surrounding scenery, but instead captures a solid color image. For example, if an intruder covers all or part of camera's lens, a blind camera alarm may be generated.

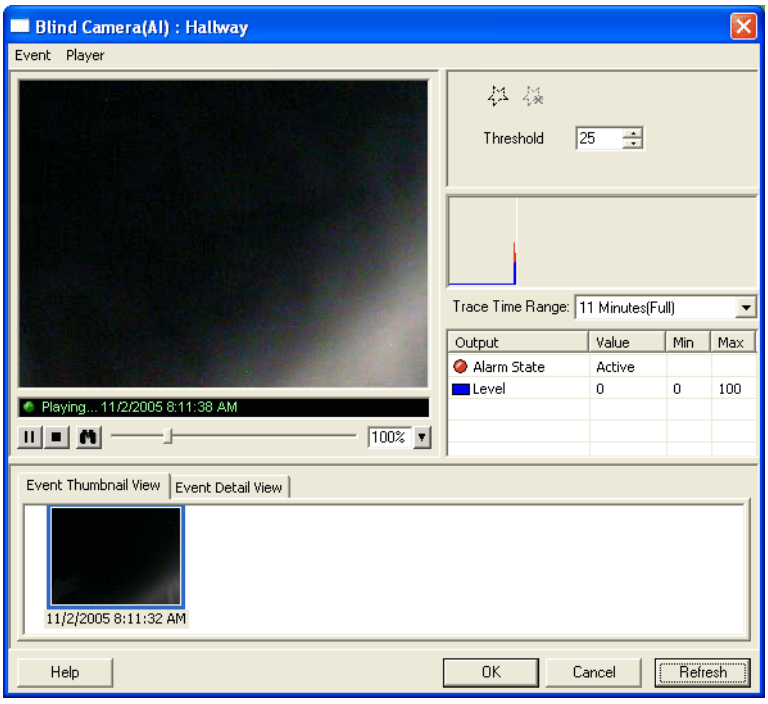
Note: LNVR with firmware version 1.31 and greater support motion detection and blind camera image processing.

Blind camera detection applies to cameras configured with LDVR or LNVR recorders. However, there are subtle differences in the user's ability to configure blind camera settings, as well as differences when a recorder generates a blind camera alarm.

- LDVR-SP, LDVR-SP30, and LDVR-444 recorders - the blind camera feature is configured on the Communication sub-tab of the Camera form. Only the timezone when the blind camera detection applies is user-configurable.
- LNVR recorders - the blind camera feature is configured on the Video Processing form. The timezone, recording frame rate, whether an alarm displays in Alarm Monitoring, and the blind camera threshold are user-configurable.

Event Configuration/Search Dialog

The Event Configuration/Search dialog allows the user to configure video processing events on IP cameras. The Event Configuration/Search dialog is opened from the Video Processing form by pressing the button during Blind Camera (AI) event configuration. For more information, refer to Event Configuration/Search Dialogs on page 1023.



Region of Interest

Region of Interest (ROI) identifies the area of video to be processed. Click the Create Region of Interest button and then click on the video to mark the area you wish to define.

Once the ROI has been created, use the mouse to drag and drop any of the green vertices or the entire ROI if adjustments are necessary. To remove an ROI, click the Delete Last Region of Interest button .

Threshold

Level of change required to generate an alarm.

Automatic Gain Control

A recorder generates blind camera detection/restored alarms under different circumstances, depending on the type of camera configured with it.

- Cameras without automatic gain control:
  - Generate blind camera detection alarms when the camera is covered and the recorder receives a solid color image.
  - Generate blind camera restored alarms when the camera is uncovered and the recorder receives images of the scene.
- Cameras with automatic gain control generate blind camera detection/restored alarms depending on the blind camera threshold as well as the camera's frame rate and speed of adjustment to changes in light conditions.

Cameras with automatic gain control automatically adjust their sensitivity level to obtain the best image quality for the current environment. If a camera is covered, its ability to adjust to its new environment and see something, as well as its frame rate determines whether a blind camera section/restored alarm occurs.

The following situations trigger blind camera detection alarms with automatic gain control cameras:

- If a camera is covered such that the automatic gain control cannot adjust to distinguish (see) the cover. This situation would occur if the cover was made of a material such that the amount of light that filters through the lens is not enough for the camera to see the cover and therefore the recorder receives at least one solid color image.
- If a camera is covered and the automatic gain control cannot adjust to distinguish (see) the cover in a timely manner (it is too slow). This situation would occur if the frame rate is fast enough that at least one solid color image is received by the recorder.
- If a camera is uncovered and it slowly adjusts the sensitivity level such that a time period occurs where the camera sees a solid color image instead of the scene. A blind camera detection alarm would be generated until the camera finishes adjusting the sensitivity. This situation would occur if the camera's speed of automatic gain control is slow enough that at least one solid image is received by the recorder. This situation would also occur it the camera has a high frame rate.

Cameras with automatic gain control may generate anywhere from zero to two blind camera detection/restored pairs of alarms during any one incidence of covering/uncovering a camera. The frame rate and speed that the camera is able to adjust itself, if at all, determines the number of pairs of alarms that occur in one incidence. Refer to the following sequence of events:

1. A camera is covered.
2. Depending on the camera's frame rate/speed, the recorder may send a blind camera alarm.
   - If an alarm was issued and the camera was able to readjust itself to see something between the lens and the cover, the recorder generates a blind camera restored alarm.

- Otherwise, the blind camera restored alarm will not be generated until the cover is removed.

When the cover is removed, regardless of what happened in the previous step, the recorder might send a blind camera alarm, depending on the adjustment speed and frame rate of the camera, if it sees white.

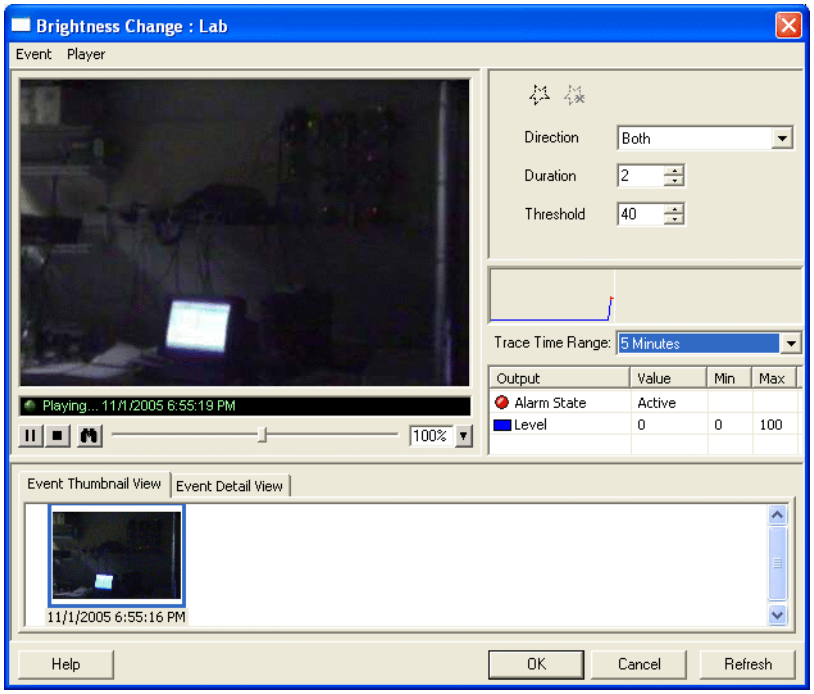
If the recorder sent a blind camera alarm, it will send a blind camera restored alarm when the camera readjusts itself to the surrounding light conditions.

Brightness Change

Brightness change detection generates an alarm when there is a change in the lighting in a scene.

Event Configuration/Search Dialog

The Event Configuration/Search dialog allows the user to configure video processing events on IP cameras. The Event Configuration/Search dialog is opened from the Video Processing form by pressing the button during Brightness Change event configuration. For more information, refer to Event Configuration/Search Dialogs on page 1023.



Region of Interest

Region of Interest (ROI) identifies the area of video to be processed. Click the Create Region of Interest button and then click on the video to mark the area you wish to define. Once the ROI has been created, use the mouse to drag and drop any of the green vertices or the entire ROI if adjustments are necessary. To remove an ROI, click the Delete Last Region of Interest button .

Direction

Set the type of brightness changes that will generate an alarm. Options are brightness increased, brightness decreased, or both.

Duration

Length of time (in seconds) that the alarm will remain active after detecting a change in brightness. If the event is not restored within this time, the new brightness level will become the base level from which future alarms are generated.

Threshold

Level of change required to generate an alarm.

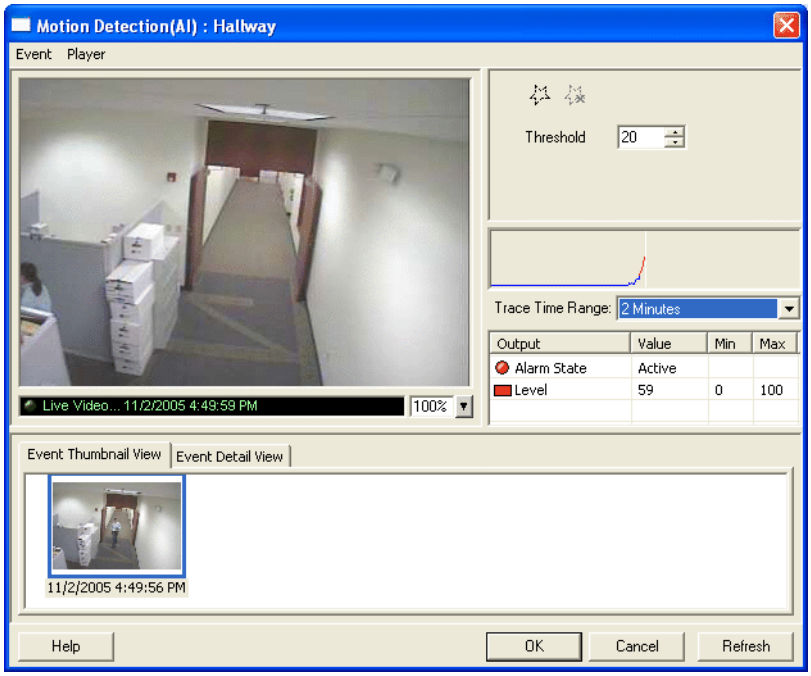
Motion Detection (AI)

The motion detection feature applies to cameras configured with LNVS, LNVR, LDVR-SP, LDVR-SP30, LDVR-408, and LDVR-444 recorders.

- For LNVS, LDVR-SP, LDVR-SP30,LDVR-408, and LDVR-444 recorders, the timezone for motion detection is set using options on the **Communication** sub-tab of the **Camera** form.
- For LNVR recorders, the timezone, frame rate, and threshold for motion detection are configured on this form.

Event Configuration/Search Dialog

The Event Configuration/Search dialog allows the user to configure video processing events on IP cameras. The Event Configuration/Search dialog is opened from the Video Processing form by pressing the button during Motion Detection (AI) event configuration.



Region of Interest

Region of Interest (ROI) identifies the area of video to be processed. Click the Create Region of Interest button and then click on the video to mark the area you wish to define. Once the ROI has been created, use the mouse to drag and drop any of the green vertices or the entire ROI if

adjustments are necessary. To remove an ROI, click the Delete Last Region of Interest button .

Threshold

Level of change required to generate an alarm.

Embedded IntelligentVideo Events

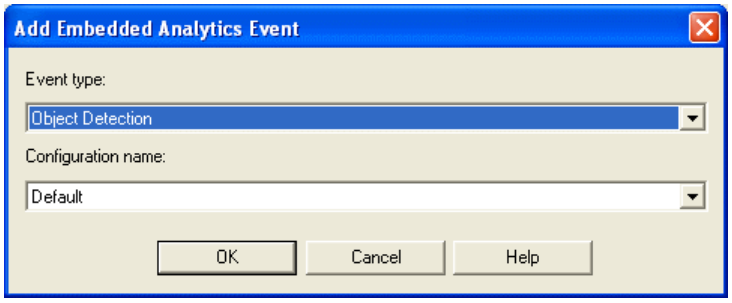
Embedded IntelligentVideo supports camera processing of several events. Each of these events is explained in detail in the user guides of the cameras that support them.There is a limit on how many algorithms can be configured per channel. You can have one instance of Smart VMD and Invalid Camera on each channel. In addition, you can have one instance of either Object Detection or Loitering. There should only be a maximum of three events per channel.

Note: The embedded analytics configuration for a camera can only be modified by one user at a time. If another user attempts to edit the configuration while a modification is in progress, an error message will be displayed.

Maximum Number of Embedded Algorithms per Channel

Option	Smart VMD	Invalid Camera	Object Detection	Loitering
1	X	X	X	
2	X	X		X

Embedded Analytics Configuration Wizard



The Embedded Analytics Configuration Wizard is used to create a new Embedded Analytics Event. Once the event has been created with the wizard it can be edited using the Event Configuration/ Search dialog.

Event Type

Select the embedded analytics event you want to configure from the drop-down. Only the embedded analytics events supported by the currently selected camera will be displayed in the drop-down.

Configuration name

Select the configuration type you want to configure from the drop-down. Only the configuration types supported by the currently selected camera and **Event Type** will be displayed in the drop-down.

Each event supports a Default configuration type, which is not designed for a specific scenario. The Default configuration type is selected by default.

OK

Saves the selected **Event Type** and **Configuration Type** as an embedded analytics event on the camera and closes the Embedded Analytics Configuration Wizard.

Cancel

Closes the Embedded Analytics Configuration Wizard without saving any changes to the camera.

Embedded Event Configuration Types

Each Embedded Analytics event has pre-configured options available in the Embedded Analytics Configuration Wizard. Each event has a “Default” configuration type which is not designed for a specific scenario. This Default configuration type is selected by default in the wizard.

Invalid Camera

The Invalid Camera embedded event has the following configuration options available:

- Light Version. Used in cases that require high processing throughput (high number of cameras per server).

Loitering

The Loitering embedded event has the following configuration options available:

- Outdoors. For use outdoors and for indoor scenes with outdoor light sources. Behaves similarly to Stable Indoors.
- Stable Lighting, Indoors. For use with indoor scenes containing no outdoor light sources. In this scenario a human that is loitering for at least 30 seconds is detected. The view of the camera is limited such that the human should occupy at least 600 pixels in the image plane.

Object Detection

The Object Detection embedded event has the following configuration options available:

- Intrusion Detection - General Object. Detects any object.
- Intrusion Detection - Human Intruder. Detects humans.

Smart VMD

The Smart VMD embedded event has the following configuration options available:

- Stable Lighting, Indoors. Used to detect motion in very controlled scenarios with stable lighting and no camera vibration.
- Unstable Lighting, Indoors. Used to detect motion in scenarios in which no camera vibration is expected, but lighting is subject to changes (due to window exposure, etc.). The Level of Change must exceed the configured threshold for a duration of at least 2 seconds to generate an alarm.

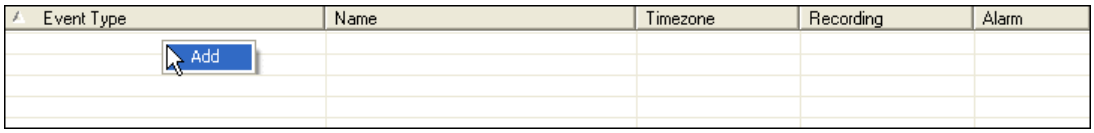
- Low-light, Stable Camera. Used to detect motion in scenarios with low lighting levels and no camera vibration. The Level of Change must exceed the configured threshold for a duration of at least 2 seconds to generate an alarm.
- Outdoors, Unstable Camera. Used to detect motion in scenes where camera vibration is possible and frequent changes in lighting are likely. The Level of Change must exceed the configured threshold for a duration of at least 2 seconds to generate an alarm.

Video Processing Form Procedures

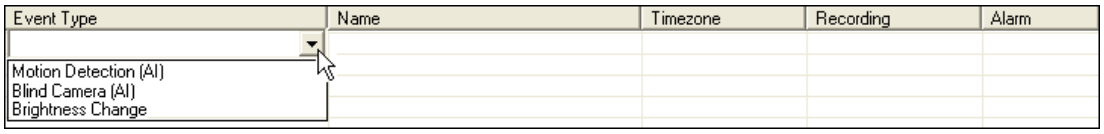
Add Event Settings

Complete the following procedure to configure motion detection, blind camera or brightness changes for cameras with LNVR recorders.

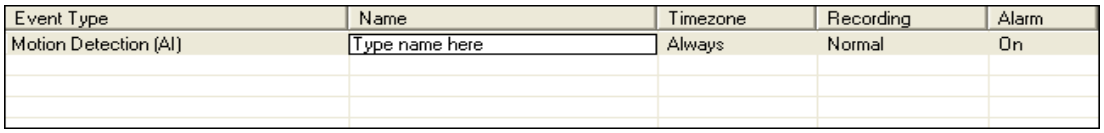
1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Video Processing tab.
3. Select (place a check mark beside) the appropriate camera.
4. Click [Modify].
5. With your cursor in the Event Type column, right-click and select "Add".



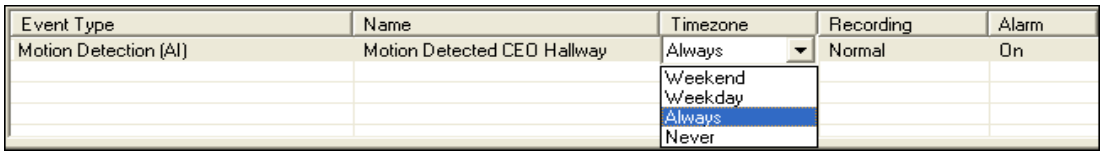
6. Select the event type from the drop-down.



7. Select the field that displays under the Name column. Enter a descriptive name that will be appended to the alarm description in Alarm Monitoring (when this event occurs).



8. Select the field in the Timezone column. A drop-down displays. Select the timezone during which the settings apply.



9. Select the field in the Recording column. A drop-down displays. Select the type of recording settings to use.
10. Select the field in the Alarm column. A drop-down displays. Select whether an alarm will display in Alarm Monitoring or not.

11. To configure event specific properties, click the camera icon to the right of the Alarm column.
12. The Event Configuration/Search Dialogs is displayed. Refer to the section for specific event information you are configuring for more information.
13. Repeat steps 5 through 12 for each new event you want for the specified camera.
14. Click [OK].

Import Event Settings

Note: To import embedded analytics events, the embedded firmware version on the camera must match the firmware version of the imported event.

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Video Processing tab.
3. Select (place a check mark beside) the camera you wish to import event settings to.
4. Click [Modify].
5. Right-click in the camera list view and select **Import event(s)**.
6. Browse for the configuration file (*.xml) and click [Open].
7. Click [OK] to save the camera configuration.

Export Event Settings

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Video Processing tab.
3. Select (place a check mark beside) the camera you wish to export event settings from.
4. Right-click the camera in the list view and select **Export event(s)**.
5. Save the configuration file (*.xml).

Add Embedded Analytics

1. From the ***Video*** menu, select ***Digital Video***. The Digital Video folder opens.
2. Click the Video Processing tab.
3. Select (place a check mark beside) the appropriate camera.
4. Click [Update Capabilities] to verify that Embedded Analytics are supported for the selected camera.
5. Click [Modify].
6. Click [Add Embedded Analytics Event].
7. Select the embedded analytics event you want to configure from the **Event type** drop-down.
8. Select the configuration type you want to configure from the **Configuration name** drop-down.
9. Click [OK] to save the Embedded Analytics Event.
10. Click [OK] to save the camera settings.

CHAPTER 49

IntelligentVideo Folder

To configure OnGuard IntelligentVideo, you must configure the IntelligentVideo Server (IVS) as well as the events. The IVS is configured on the IntelligentVideo Server form in System Administration. Events are configured on the Event Configuration/Search dialog, which is opened through the IntelligentVideo Event form or the Video Player in System Administration.

In addition to events, you can configure channel parameters for the video channel itself. Channel parameters are configured on the Video Channel Configuration dialog.

The recommended configuration sequence in the OnGuard software is:

1. Configure an IntelligentVideo Server. For more information, refer to Configure an IntelligentVideo Server on page 1012.
2. Configure a video recorder. For more information, refer to Add LNVR Video Recorders on page 933.
3. Configure cameras. For more information, refer to Configure LNVR Cameras on page 962.
4. Configure IntelligentVideo event settings. For more information, refer to IntelligentVideo Events Form Procedures on page 1014.

The folder contains the following forms: the IntelligentVideo Server form, the IntelligentVideo Events form, the IntelligentVideo Application form, and the IntelligentAudio form.

You can display the IntelligentVideo folder by selecting ***IntelligentVideo*** from the ***Video*** menu. or by selecting the IntelligentVideo toolbar button.

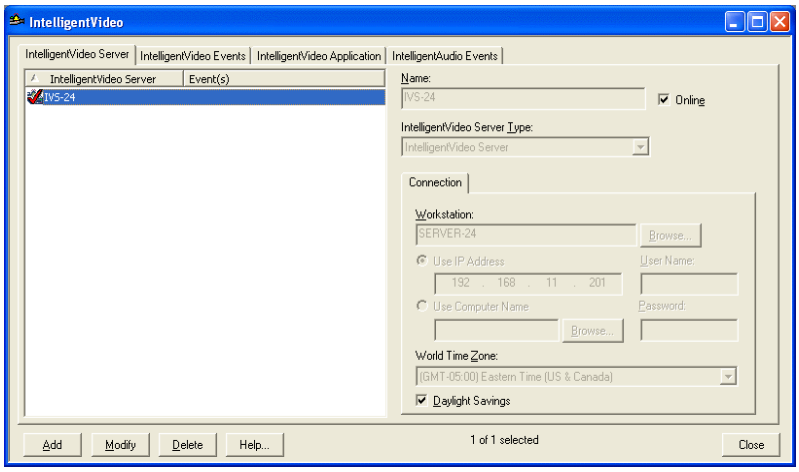
Toolbar Shortcut

For detailed IntelligentVideo Event configuration information, refer to the IntelligentVideo User Guide.

IntelligentVideo Server Form

The IntelligentVideo Server (IVS) is a server designed to run complex video algorithms for video processing of events. You can configure events from any video recorder to be processed using the IVS. After events are detected and processed, the IVS sends alarms to Alarm Monitoring.

For detailed IntelligentVideo Event configuration information, refer to the IntelligentVideo User Guide.



Listing window

Lists currently defined IntelligentVideo Servers (IVS) and the total number of events configured on each server.

Name

A descriptive name for the IVS server.

Online

If selected, the IVS will be online and the Communication Server will attempt to communicate with it.

IntelligentVideo Server Type

Select the server type from the drop-down list.

Workstation

The name of the workstation the IVS connects to.

Use IP Address

Select this radio button if you want to use the IP address of the IVS. This is the address OnGuard will use to communicate with the IVS.

Use Computer Name

Select this radio button if you want to use the computer name of the IVS. This is the name OnGuard will use to communicate with the IVS.

Browse

Click this button to browse for the IVS computer name or workstation.

User Name and Password

Enter the user name and password for the specific Windows account used by OnGuard to connect with the IVS. If you leave these fields blank, OnGuard will use the interactive user Windows account. It is recommended that only users with knowledge of Windows networking and security configure these fields.

World Time Zone

The world time zone for the geographical location of the IVS. The selections in the drop-down list are sequential and each include:

- The world time zone's clock time relative to Greenwich Mean Time. (e.g. "GMT +05:00" indicates that the clock time for the selected IVS is 5 hours ahead of the Greenwich Mean Time.
- The name of one or more countries or cities that are located in that world time zone.

Daylight Savings

Select this check box if the IVS is located in a location that utilizes daylight savings.

Add

Adds the IVS to the system.

Modify

Changes the connection settings or IVS name for the selected servers.

Delete

Removes the IVS from the system.

Help

Displays online help for this topic.

Close

Closes the IntelligentVideo folder.

Performing a Download to the IntelligentVideo Server

A download to the IntelligentVideo Server should be performed after each of the following circumstances has occurred:

- The IVS has been marked offline, and has been brought online again.
- Whenever a new IVS is added to the system.
- Whenever the IVS is upgraded.
- The system has been converted to a segmented system.
- When failover settings have been changed on a camera channel that has IntelligentVideo events configured.

To perform a download, right-click the IVS and select **Download**.

IntelligentVideo Server Form Procedures

Use the following procedures on this form.

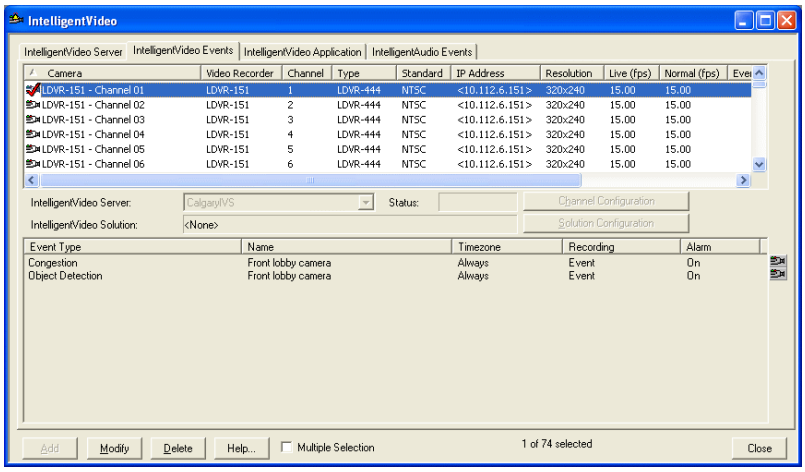
Configure an IntelligentVideo Server

1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentVideo Server tab.
3. Click [Add].
4. Enter a name for the IVS.
5. Select **IntelligentVideo Server** or **IntelligentVideo Application Server** from the **IntelligentVideo Server Type** drop-down list.
6. Identify how the IVS will communicate with the recorder, by entering the workstation, and IP address or computer name of the IVS.
7. Enter the user name and password for the specific Windows account used by OnGuard to connect with the IVS, or use the default values.
8. Select the world time zone for the geographical location of the selected IVS.
9. Select the **Daylight Savings** check box if you want to properly convert between various time formats for daylight savings.
10. Click [OK].
11. The Monitor Zone Assignments window is displayed. Select the monitor zone(s) you wish to assign the server to and click [OK].

IntelligentVideo Events Form

The IntelligentVideo Events form applies to cameras configured with any video recorder. This form allows you to configure multiple events or one solution for a camera to be processed on a specified IVS server only. Additional licensing (Maximum Number of IntelligentVideo Streams) is required to use IntelligentVideo processing.

In addition to events, you can configure channel parameters for the video channel itself. The IntelligentVideo form includes a [Channel Configuration] button which allows you to configure channel parameters. For more information, refer to Video Channel Configuration Dialog on page 1032.



For detailed IntelligentVideo Event configuration information, refer to the IntelligentVideo User Guide. For detailed IntelligentVideo Solution configuration information, refer to the IntelligentVideo Solutions User Guide.

Camera listing window

Lists currently defined IP cameras and the recorders they are associated with, as well as the channel, camera type, video standard, camera IP address, camera resolution, and IVS that will process data for specific events.

IntelligentVideo Server

Select the name of the IVS server for the selected camera.

IntelligentVideo Solution

Lists the name of the IVS solution loaded on the camera.

Status

Displays the status of the selected IVS.

Channel Configuration

Click this button to display the Video Channel Configuration dialog. The Video Channel Configuration dialog is used to configure event parameters that apply to the entire video channel and not the individual video processing algorithms. The [Channel Configuration] button activates when System Administration successfully connects to the selected IVS. Click this button to display the Video Channel Configuration dialog.

You can also display the Video Channel Configuration dialog through a [Channel Configuration] button on the Event Configuration/Search dialog. For more information, refer to Video Channel Configuration Dialog on page 1032.

Solution Configuration

Click this button to access the Solution Configuration menu. Use this menu to **Add**, **Modify**, **Delete**, or **Convert Separate Events**. The **Add** and **Modify** menu options launch the Solution Configuration wizard. To stop using a solution while retaining configured events, select the ***Convert Separate Events*** menu option. This option allows the user control over parameters that are pre-configured as part of the solution.

Event Type

Displays the name of the configured event. For more information, refer to the IntelligentVideo Event chapters in the IntelligentVideo User Guide.

Name

A descriptive name for the event that will display in Alarm Monitoring. The name can be 21 characters long. Since OnGuard supports two events of the same type, for the same camera, the name should be descriptive enough for Alarm Monitoring operators to recognize where the event occurred.

Timezone

The timezone during which the specified IntelligentVideo setting is active. Timezones are created on the Timezones folder, which is located by selecting ***Timezone*** from the ***Access Control*** menu.

Recording

The type of recording that will be used. Choices include:

- **Event** - increased frame rate with pre-roll for OnGuard specific events. Event recording settings are configured on the Event Mode sub-tab of the Camera form.
- **Normal** - continuous or time-lapsed recording. Normal recording settings are configured on the Normal Mode sub-tab of the Camera form.

Alarm

Determines whether an alarm displays in Alarm Monitoring.

- **On** - If the threshold is reached during the selected timezone, an alarm is sent from the recorder to OnGuard and an alarm displays in Alarm Monitoring.
- **Off** - If the threshold is reached during the selected timezone an alarm will not be active (sent to OnGuard) nor will it display in Alarm Monitoring.

Displays the Event Configuration/Search Dialog where you can configure event-specific parameters. For more information, refer to Event Configuration/Search Dialogs on page 1023.

Modify

Changes the IntelligentVideo settings for the selected camera.

Delete

Deletes all configured events for the selected camera. Only the [Delete] button can be used with the **Multiple Selection** check box.

Help

Displays online help for this topic.

Multiple Selection

Select this check box to select multiple entries in the listing window. Multiple selection only applies to the delete option.

Close

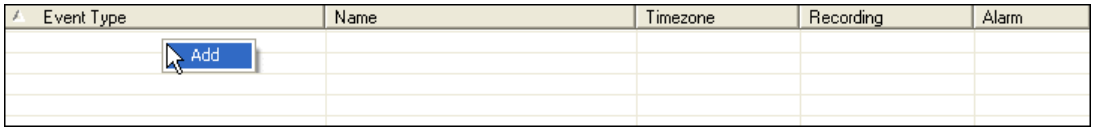
Closes the IntelligentVideo folder.

IntelligentVideo Events Form Procedures

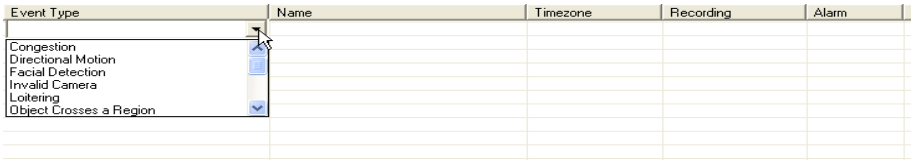
Use the following procedures on this form.

Add IntelligentVideo Event Settings

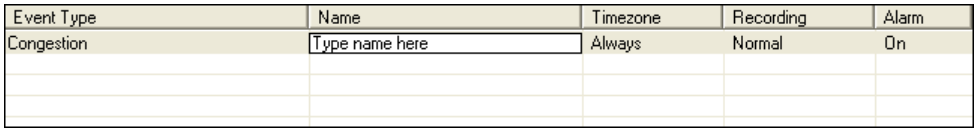
1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentVideo Events tab.
3. Select (place a checkmark beside) the appropriate camera.
4. Click [Modify].
5. Select the IVS that will process images for the events.
6. With your cursor in the Event Type column, right-click and select **Add**.



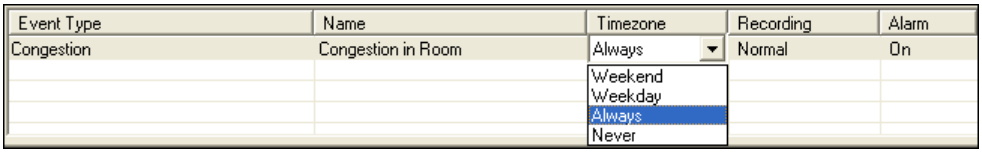
7. Select the event type from the drop-down list.



8. Select the field that displays under the Name column. Enter a descriptive name that will be appended to the alarm description in Alarm Monitoring (when this event occurs).



9. Select the field in the Timezone column. A drop-down list displays. Select the timezone during which the IntelligentVideo settings apply.



10. Select the field in the Recording column. A drop-down list displays. Select the type of recording settings to use.
11. Select the field in the Alarm column. A drop-down list displays. Select whether an alarm will display in Alarm Monitoring or not.
12. To configure event specific parameters, click the camera icon to the right of the Alarm column.For more information, refer to Event Configuration/Search Dialogs on page 1023.
13. To configure channel parameters for the video channel itself, click [Channel Configuration]. For more information, refer to Video Channel Configuration Dialog on page 1032.
14. Repeat steps 5 through 12 for each new event you want for the specified camera.
15. Click [OK].

Modify IntelligentVideo Settings

1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentVideo Events tab.
3. Select (place a checkmark beside) the appropriate camera.
4. Click [Modify].
5. Select a field in any of the columns.
6. Change the settings.
7. Click [OK].

Delete IntelligentVideo Settings

1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentVideo Events tab.
3. Select (place a checkmark beside) the appropriate camera.
4. Click [Delete].

5. Click [OK].

Copy and Paste Event Settings

1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentVideo Events tab.
3. Right-click the camera with the event settings you wish to copy and select **Copy Event(s)**.
4. Select (place a checkmark beside) the camera you wish to paste the event settings to.

Note: To paste the event settings to multiple cameras, select the **Multiple Selection** check box, then select the additional cameras.

5. Right-click one of the selected cameras and select **Paste Event(s)** to paste all of the event settings or **Paste Special** to choose which events to paste and whether to include the channel configuration.

Import Event Settings

1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentVideo Events tab.
3. Select (place a checkmark beside) the camera you wish to import event settings to.
4. Click [Modify].
5. Select the **IntelligentVideo Server** from the drop-down list.
6. Right-click in the camera list view and select **Import event(s)**.
7. Browse for the configuration file (*.xml) and click [Open].

Export Event Settings

1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentVideo Events tab.
3. Select (place a checkmark beside) the camera you wish to export event settings from.
4. Right-click the camera in the list view and select **Export event(s)**.
5. Save the configuration file (*.xml).

Add an IntelligentVideo Solution

For more information, refer to the IntelligentVideo Solutions User Guide.

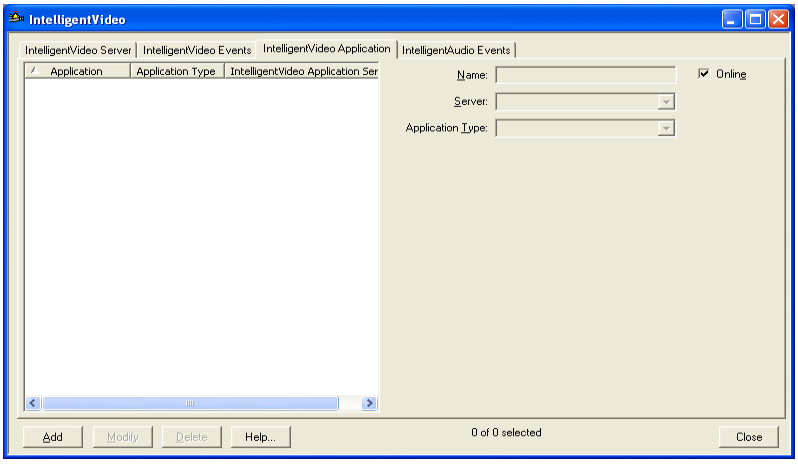
1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentVideo Events tab.
3. Select (place a checkmark beside) the appropriate camera.
4. Click [Modify].
5. Select the IVS that will process images for the solution.
6. Click [Solution Configuration] and select and select **Add Solution** from the pop-up menu.
7. The Solution Configuration wizard is displayed. Select the desired solution from the **IntelligentVideo Solution Type** drop-down list and click [Next >].
8. Select the **Configuration Type** corresponding to the scene from the drop-down list.

9. An instance of the solution is created in the list view. The list view is used to configure a name for the alarm, set the timezone for alarm generation, and optionally configure the Out of Focus or Out of Home Position settings.
10. Click [Finish] to create the IntelligentVideo Solution Configuration.
11. Click [OK] to save the configuration.

IntelligentVideo Application Form

The IntelligentVideo Application Server (IV App Server) is a service whose main purpose is to provide a host environment for individual IntelligentVideo applications. The IV App Server performs the following functions:

- Provides a means to dynamically add and remove IntelligentVideo applications.
- Provides functionality common to all application such as error login, data, and configuration persistence and communications.
- Provides a base on which any number and wide range of applications can be supported in the future.



Note: Detailed configuration options appear after an application type has been selected from the drop-down list. For more information, refer to the IntelligentVideo Application Server User Guide.

Listing window

Lists currently defined applications with the type and server name.

Name

A descriptive name for the application.

Online

If selected, the application will be online and the Communication Server will attempt to communicate with the application.

Server

Select the IntelligentVideo Application Server from the drop-down list.

Application Type
Select the type of application from the drop-down list.

Add
Adds an application to the system.

Modify
Changes the configuration of the application.

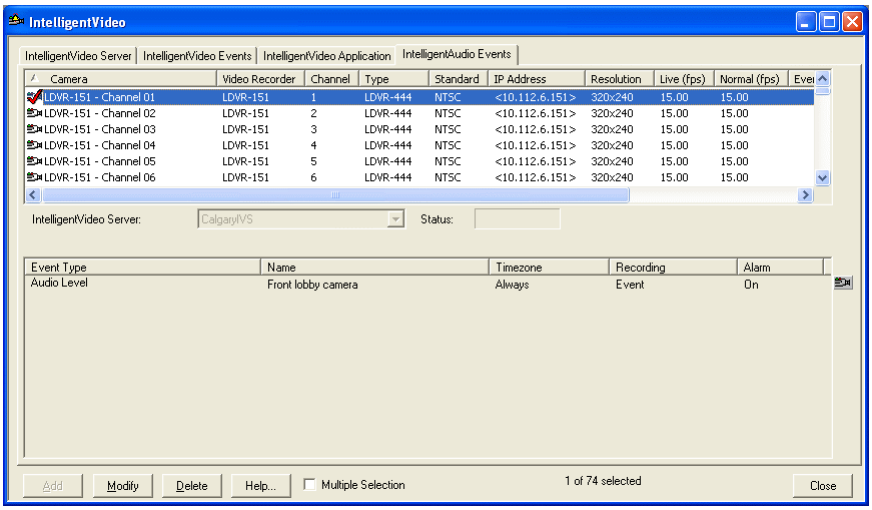
Delete
Removes the application from the system.

Help
Displays online help for this topic.

Close
Closes the IntelligentVideo folder.

IntelligentAudio Events Form

The IntelligentAudio Events form is used to configure events to trigger alarms in Alarm Monitoring. Currently only the Audio Level event is supported for generating alarms. Additional audio events can be used for forensic processing. For more information, refer to the Digital Video Software User Guide.



Camera listing window
Lists currently defined IP cameras and the recorders they are associated with, as well as the channel, camera type, video standard, camera IP address, camera resolution, and IVS that will process data for specific events.

IntelligentVideo Server
Select the name of the IVS server for the selected camera.

Status
Displays the status of the selected IVS.

Event Type
Displays the name of the configured event.

Name
A descriptive name for the event that will display in Alarm Monitoring. The name can be 21 characters long. Since OnGuard supports two events of the same type, for the same camera, the name should be descriptive enough for Alarm Monitoring operators to recognize where the event occurred.

Timezone
The timezone during which the specified event is active. Timezones are created on the Timezones folder, which is located by selecting ***Timezone*** from the ***Access Control*** menu.

Recording
The type of recording that will be used. Choices include:

- **Event** - increased frame rate with pre-roll for OnGuard specific events. Event recording settings are configured on the Event Mode sub-tab of the Camera form.
- **Normal** - continuous or time-lapsed recording. Normal recording settings are configured on the Normal Mode sub-tab of the Camera form.

Alarm
Determines whether an alarm displays in Alarm Monitoring.

- **On** - If the threshold is reached during the selected timezone, an alarm is sent from the recorder to OnGuard and an alarm displays in Alarm Monitoring.
- **Off** - If the threshold is reached during the selected timezone an alarm will not be active (sent to OnGuard) nor will it display in Alarm Monitoring.

Displays the Event Configuration/Search Dialog where you can configure event-specific parameters. For more information, refer to Event Configuration/Search Dialogs on page 1023.

Modify
Changes the event settings for the selected camera.

Delete
Deletes all configured events for the selected camera. Only the [Delete] button can be used with the **Multiple Selection** check box.

Help
Displays online help for this topic.

Multiple Selection
Select this check box to select multiple entries in the listing window. Multiple selection only applies to the delete option.

Close
Closes the IntelligentVideo folder.

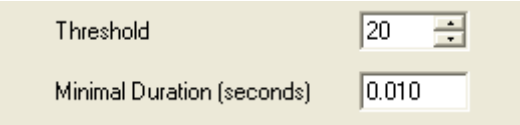
Audio Level Event

The Audio Level event identifies sound events crossing a volume threshold.

Event Properties

The event properties are defined from the Event Configuration/Search dialog which is launched with the camera icon on the IntelligentAudio Events form during event configuration. For more information, refer to Event Configuration/Search Dialogs on page 1023.

Note: IntelligentAudio events do not have a region of interest or channel parameters.



Threshold

Volume threshold for detection. Use the level displayed on the Event Feedback pane to determine a value appropriate to the scene.

Minimal Duration (seconds)

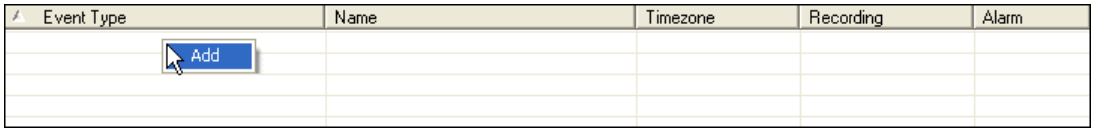
Length of time that sound should continue before an event is detected. The range of values is 0.010 to 10.000 seconds.

IntelligentAudio Events Form Procedures

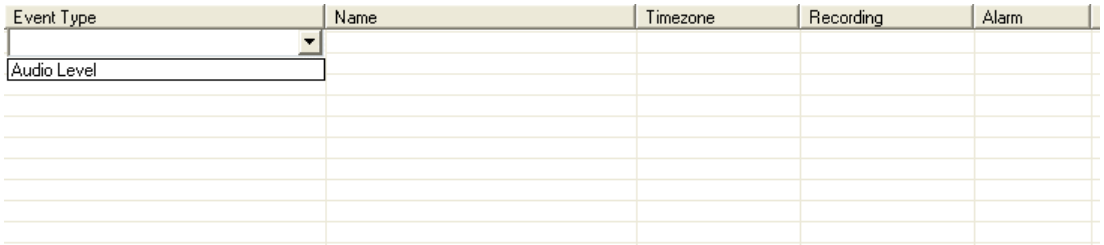
Use the following procedures on this form.

Add IntelligentAudio Event Settings

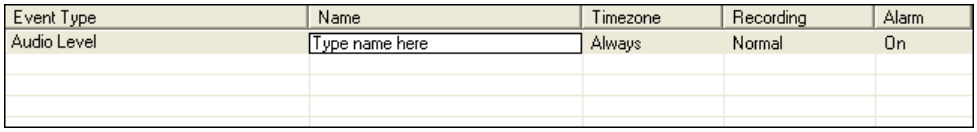
1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentAudio Events tab.
3. Select (place a checkmark beside) the appropriate camera.
4. Click [Modify].
5. Select the IVS that will process images for the events.
6. With your cursor in the Event Type column, right-click and select **Add**.



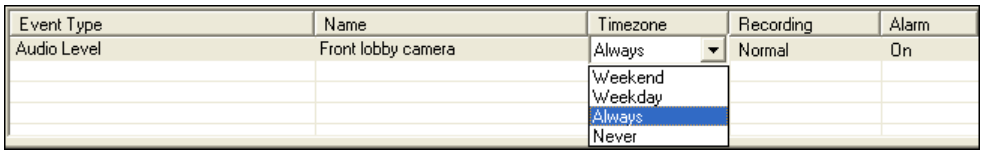
7. Select the event type from the drop-down list.



8. Select the field that displays under the Name column. Enter a descriptive name that will be appended to the alarm description in Alarm Monitoring (when this event occurs).



9. Select the field in the Timezone column. A drop-down list displays. Select the timezone during which the IntelligentAudio settings apply.



10. Select the field in the Recording column. A drop-down list displays. Select the type of recording settings to use.
11. Select the field in the Alarm column. A drop-down list displays. Select whether an alarm will display in Alarm Monitoring or not.
12. To configure event specific parameters, click the camera icon to the right of the Alarm column.For more information, refer to Event Configuration/Search Dialogs on page 1023.
13. Click [OK].

Modify IntelligentAudio Settings

1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentAudio Events tab.
3. Select (place a checkmark beside) the appropriate camera.
4. Click [Modify].
5. Select a field in any of the columns.
6. Change the settings.
7. Click [OK].

Delete IntelligentAudio Settings

1. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
2. Click the IntelligentAudio Events tab.
3. Select (place a checkmark beside) the appropriate camera.
4. Click [Delete].
5. Click [OK].

CHAPTER 50

Event Configuration/Search Dialogs

The Event Configuration/Search dialog is used to:

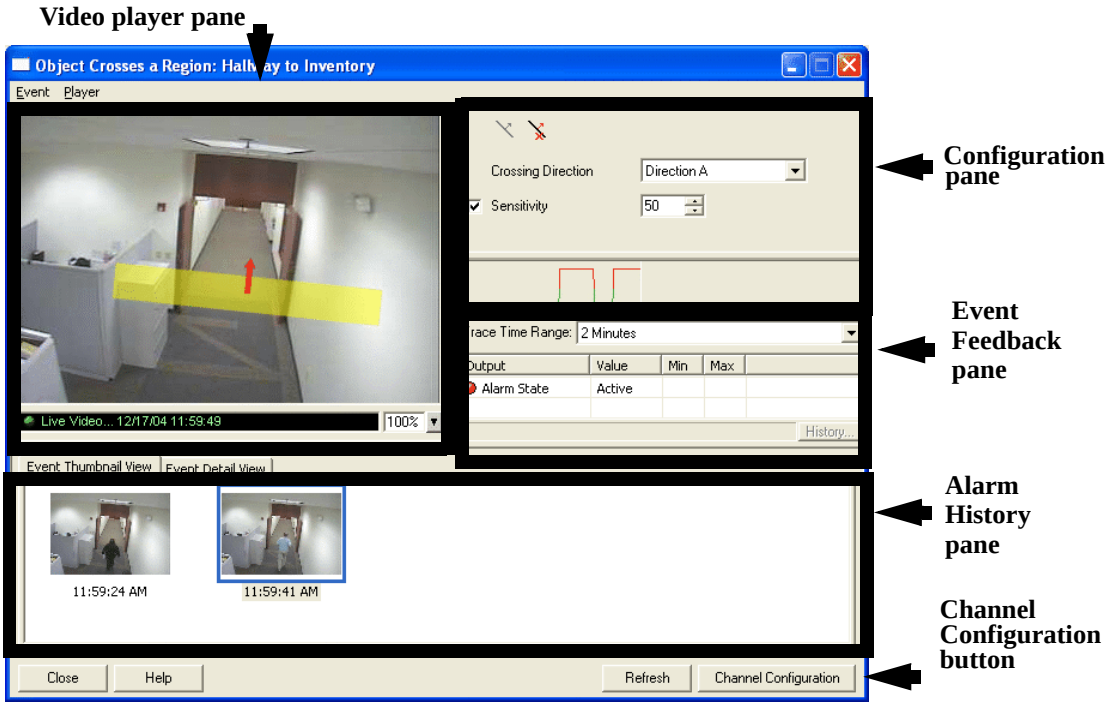
- Configure event parameters for real-time video processing and alarm generation. This includes motion detection, blind camera and brightness changes as well as events for IntelligentVideo, and IntelligentAudio processing.
- Display alerts when events occur. Alerts display in three areas of the dialog:
  - In the video window, alerts display as a highlighted area.
  - In the Event Feedback pane, alerts display as a spike in the alert status graph.
  - In the alarm history pane, alerts display as thumbnails or text.
- Search LNVR recorded/archived video for the occurrence of specific events.
- View search results as a detailed list or thumbnail images.
- Play recorded video search results in the Video Player pane.
- Play live video in the Video Player pane.

The Event Configuration/Search dialog can be used with the following video sources:

- Live video
- Recorded video, accessed through a video recorder
- Exported video files

IMPORTANT: Cameras that support embedded IntelligentVideo events should not have camera image rotation configured in System Administration. The configuration is not be rotated when it is sent to the camera, and if embedded IntelligentVideo events are configured in OnGuard with the image rotated

When playing exported video over a network, the Windows account that the LpsSearchSvc service runs under must have permission to access the files.



Different fields, buttons and event options are available, depending on how you open the Event Configuration/Search dialog.

Event Configuration/Search Dialog Menu Options

The following table describes the menu and sub-menu options available from the Event Configuration/Search dialog.

Event Menu

Select Event

Enables you to select the event for which the current video source will be analyzed. The ***Select Event*** sub-menu option is available only if you open the Event Configuration/Search dialog using the Video Player.

In System Administration, you have to select an event before you can open the Event Configuration/Search dialog. Therefore, if you selected an event to open the dialog this the ***Select Event*** sub-menu option will not display.

Screen Output

Some event feedback and configuration parameters display directly on the video to help you visualize what is being (or what has been) configured. If you wish to enable this output, verify a checkmark displays beside this sub-menu option.

Load/Save Configuration

Allows you to save the current configuration and load it at a later time for the same type of event.

Copy/Paste Configuration

It is possible to copy a configuration from one event and paste it to a different event. In this case, all parameters that apply to the new event will be used.

For example, the configuration for a motion detection event can be copied/pasted to an abandoned object event. In this example, the “Region of interest” parameter exists in both events, so that parameter will be saved. But the abandoned object event does not use “Threshold”, so that parameter will be ignored. Lastly, motion detection did not use the “Duration” parameter, so the original duration value for the abandoned object event will be used.

Show Advanced Configuration

Select this sub-menu item to view additional properties used for troubleshooting and diagnostics. These advanced properties are used for advanced calibration of events and should rarely be used.

Player Menu

Switch to Recorded/Live

Enables you to switch to and from recorded and live video.

Select Start/End Times

Displays a dialog where you can select the start and end times of a recorded video search.

Export Frame

Allows you to export the current frame into a picture file. Supported image formats are BMP, JPEG, GIF, TIFF, and PNG.

Play

Starts/resumes video playback. This command is not visible when video is playing.

Pause

Pauses playback. When video play is resumed, it continues from where it was temporarily stopped. This command is visible only when video is playing.

Stop

Stops playback and rewinds the video to the beginning.

Search

Fast-forwards through video while continuing to analyze it. This allows you to search through video faster than real-time and look for events of interest, using the Event Output and Event History panes.

Zoom

Enables you to set pre-defined (50%, 100%, and 200%) zoom levels for the video player.

Frame Rate

Sets the frame rate at which video is fed to the client side. By default, this value is set to 10 frames per second (fps). If the source video is set at a higher fps, video will be analyzed at the higher frame rate, but some frames will not be sent to the client display.

This option is available when the client display is on a computer separate from the video analysis service and the network connection between client and the service is less than ideal. Reducing the frame rate will speed up processing because the server side will not have to wait for the client to consume the video frames it has sent.

Event Configuration/Search Dialog Fields

The following table describes some of the configuration parameters available in the Event Configuration/Search dialog.

Video Player Pane

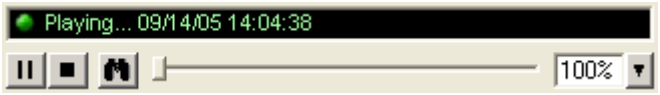
Video window

Video playback window. If configuration or event feedback controls have any additional information, you may choose to draw in this window or on top of the video.

Command buttons and Status indicator

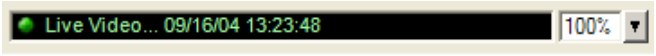
Buttons at the bottom of the pane allow you to execute the same commands that are available through the menus. In addition to the menu options, the command buttons allow you to:

- Set an arbitrary zoom level for the entire video search window
- Search video by using the position indicator/seek bar control
- Play, pause, and stop recorded video
- Play the video at an accelerated rate by using the search button



Indicates the current status of the IntelligentVideo engine or video processing engine. If there are problems connecting to the search server component, the status indicator will indicate the connection state and any error values encountered.

In live video mode, most of these controls are absent since live video cannot be paused, stopped, or searched. The only option available with live video is to change the zoom level.



Configuration Pane

The fields that display in the Configuration pane depend on the event selected. An event must be selected to populate the Configuration pane.

Region of Interest (ROI)

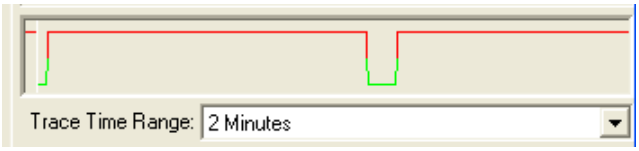
The ROI identifies the area of video to be processed. Click the **Create a Region of Interest** button and then click on the video to mark the area you wish to define. The ROI is a general polygon which can consist of a minimum of 4 and a maximum of 10 vertices. Once the ROI has been created, use the mouse to drag and drop any of the green vertices or the entire ROI if adjustments are necessary. Click the **Delete Region Of Interest** button to remove an existing ROI.

Mask

The ROI mask identifies an area of video to ignore. Click on the **Create a Mask** button and then click on the video to mark the area you wish to ignore. Once the mask has been created, use the mouse to drag and drop any of the green vertices or the entire mask if adjustments are necessary. Click the **Delete Mask** button to remove an existing mask.

Event Feedback Pane

Alert status graph

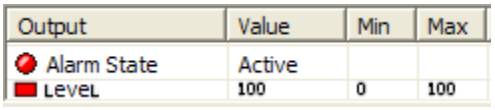


A color-coded graphical representation of alerts. An alert is created only if the last detected event occurred more than 8 seconds ago. For recorded video, you can click on any part of the graph to view the corresponding video. The video search must first be stopped.

Time Range

Select the duration of time used by the graph.

Level



The current level of change. Levels range from 0 to 100. The first and last frames of an event must have a value greater than or equal to the specified level, to be included in the search results.

Status Message Pane

Displays messages regarding the status of the background. Statuses that can be generated include:

- "Events disabled: engine initializing": Notifies that the initial background has not been acquired yet, therefore the events that require background are disabled.
- "New Background Image Acquired": Notifies that a new background model was acquired [the background model is constantly learned, and it is updated every "Background learning" (the parameter) seconds].

History

Displays the history of the status messages.

Alarm History Pane

Event Thumbnail View

Displays a scaled-down image of the video frame for each detected event. You can double-click a thumbnail to view the recorded video for that event (in the Video Player pane). The video search must first be stopped. The Event Thumbnail View does not apply to live video.

Event Detail View

Displays information (start time, end time and duration) about each event that was detected. You can double-click an event to view the recorded video for that event (in the Video Player pane). The video search must first be stopped. The Event Thumbnail View does not apply to live video.

Help

Push button
Displays online help for this topic.

Close

Push button
Closes the Event Configuration/Search dialog.

Refresh

Push button
Once the event configuration is modified, this button will be enabled and allows you to apply configuration changes.

Event Configuration/Search Dialog Procedures

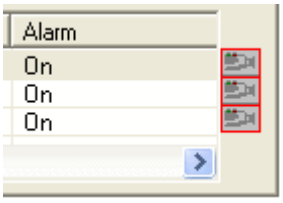
The following procedures can be performed in this dialog.

Open the Event Configuration/Search Dialog

The Event Configuration/Search dialog can be opened using the Video Processing form or IntelligentVideo Events form (in System Administration) or using the ***Video Search*** menu option (in Video Player).

Using the Video Processing or IntelligentVideo Events form

1. Open System Administration.
2. From the ***Video*** menu, select ***Digital Video or IntelligentVideo***. The Digital Video or IntelligentVideo folder opens.
3. Click the Video Processing tab or IntelligentVideo Events tab.
4. Select (place a check mark beside) the appropriate camera.
5. Click [Modify].
6. Click the camera icon located in the lower right side of the Event Type listing window. The Event Configuration/Search dialog opens.



Using the Video Player

1. Launch video from a camera using the Video Player.
2. Verify the recorded video is playing.

3. Click the Video Search toolbar button or from the ***Control*** menu select ***Video Search***. The Event Configuration/Search dialog displays.

Toolbar Shortcut

Configure Event Properties

When you configure event properties, you define the parameters that make up an event. For example, direction and object size are event properties for the Object Detection event.

Event properties are defined per event, not per channel. Therefore, you can define several unique event properties for the same event on the same video channel.

For detailed IntelligentVideo Event configuration information, refer to the IntelligentVideo User Guide.

1. Open the Event Configuration/Search dialog. For more information, refer to Open the Event Configuration/Search Dialog on page 1028.
2. If you opened the Event Configuration/Search dialog using the Video Player, select the event type from the ***Event*** menu.
3. In the Event Configuration/Search dialog, the Configuration pane displays optional and required event parameters. Some parameters require you to select a check box to enable the parameter and adjust a slider to set the value of the parameter. Other parameters display as a drop-down menu from which you select a parameter. If a button displays in the Configuration pane, then click the button to enable the feature and adjust the values of the parameter in the Video player pane. Advanced properties are displayed by selecting ***Show Advanced Configuration*** from the ***Event*** menu.For more information, refer to the IntelligentVideo User Guide.
4. Be sure to set the region of interest. For more information, refer to Set Region of Interest on page 1029.
5. If necessary, configure event parameters that apply to the video channel itself. For more information, refer to Video Channel Configuration Dialog on page 1032.
6. Click [OK].

Set Region of Interest

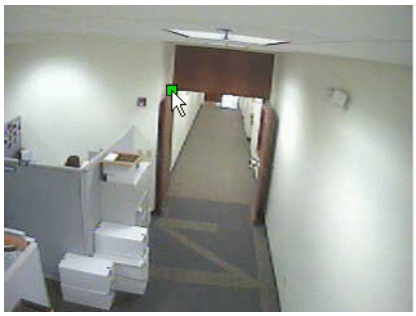
The Event Configuration/Search dialog has a region of interest (ROI) button. Although this setting is optional, it is highly recommended that ROI is used whenever possible to reduce computation time and the probability of false alarms. If the ROI is not set, the entire frame is considered the region of interest.

All the events except Object Crosses a Region and People Counting support the use of ROI.

1. Open the Event Configuration/Search dialog. For more information, refer to Event Configuration/Search Dialogs on page 1023.
2. If you opened the Event Configuration/Search dialog using the Video Player, select the event type from the ***Event*** menu.
3. Click the **Create Region of Interest** button.

Toolbar Shortcut

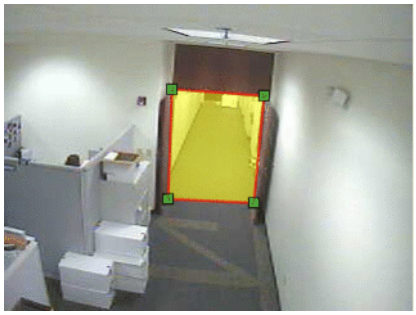
4. In the Video Player pane left-click to create a starting point for the area you want to highlight. A green dot displays.



5. Click another point in the area you want to highlight. A red line connecting the two points displays.

6. Continue clicking points to expand the highlighted area.

Note: The ROI is a general polygon which can consist of a minimum of 4 and a maximum of 10 vertices.



7. Use the mouse to drag and drop any of the green vertices or the entire ROI if adjustments are necessary.

Note: If at any time you want to remove a highlighted area, select it and click the Delete Region of Interest toolbar button.

8. Only the highlighted area is recorded or searched.

Configure Perspective Correction

The Perspective Correction mechanism is used to adjust the perceived size of an object for the 2-D image plane. It is configured on a per event basis, however once it is configured for an event it must be copied to each event on that channel that enables Perspective Size Correction. It is available for the

Object Detection, Object Left Behind, Object Removed, and Loitering events. For more information, refer to the IntelligentVideo User Guide.

1. Physically place a quadrangle object in the camera view. The quadrangle should have the following properties:
   - It must be parallel to the top and bottom of the video frame.
   - It should be a rectangle where the top and bottom lines represent the same real-world length.
   - It should be as large as possible.
2. Open the Event Configuration/Search dialog for the event.
3. From the ***Event*** menu, select ***Show Advanced Configuration***.
4. Click the **Perspective Correction for Size** button.
5. Using the mouse, right-click each of the four corners of the rectangle located on the image plane. The area selected will be displayed as a green quadrangle.

Note: When using the object size properties with the Perspective Correction mechanism, the Minimum and Maximum Object Sizes configured reflect the size of the object as it appears in the center of the ROI. If there is no ROI defined, the entire video frame is the ROI.

6. Select “Enable” from the **Use Perspective Size Correction** drop-down.

Note: Diagnostic modes are available to assist in the configuration of Perspective Correction for Size. For more information, refer to the IntelligentVideo User Guide.

7. Right-click the Configuration pane and select **Copy Configuration**.
8. In the Copy Event Configuration window, deselect any other available properties such that Perspective Correction for Size is the only property highlighted.
9. Click [OK].
10. Close the event configuration.
11. If you are configuring additional events on the same channel that will use perspective correction for size:
    a. Add the next event in the IntelligentVideo Events form and launch the Event Configuration/ Search dialog.
    b. Select “Enable” from the **Use Perspective Size Correction** drop-down.
    c. Right-click the Configuration pane and select **Paste configuration**.
    d. Finish configuring the event.
    e. Repeat steps a through d for each additional event on the channel.

Open the Video Channel Configuration Dialog

The Video Channel Configuration dialog can be opened using the Video Processing and IntelligentVideo Events forms (System Administration) or using the Event Configuration/Search dialog available through the Video Player.

Using the IntelligentVideo Events form

1. Open System Administration.
2. From the ***Video*** menu, select ***IntelligentVideo***. The IntelligentVideo folder opens.
3. Click the IntelligentVideo Events tab.

4. Select (place a check mark beside) the appropriate camera.
5. Click [Modify].
6. Select an **IntelligentVideo Server** from the drop-down list.
7. Click [Channel Configuration] (located below the camera listing window on the right side). The Video Channel Configuration dialog opens.

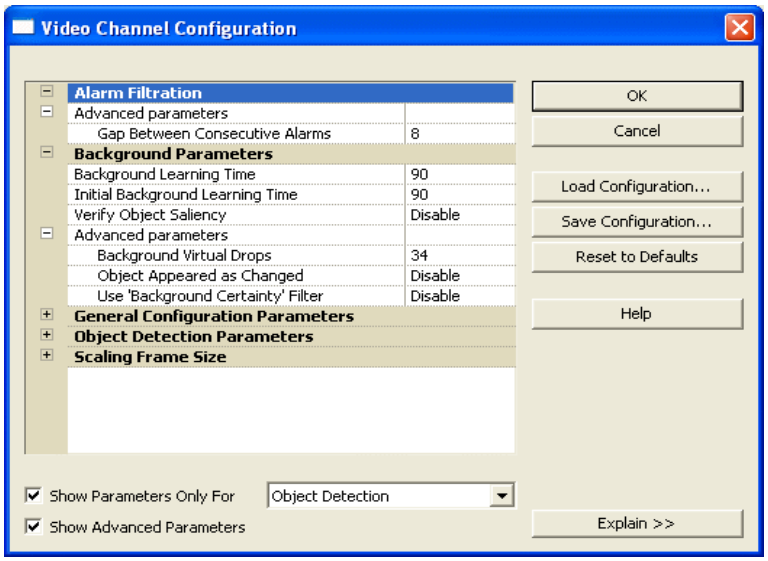
Using the Event Configuration/Search Dialog

1. Open the Event Configuration/Search dialog. For more information, refer to Open the Event Configuration/Search Dialog on page 1028.
2. Click [Channel Configuration] (located on the lower right side of the window). The Video Channel Configuration dialog opens.

Video Channel Configuration Dialog

Video channel configuration parameters can be applied to real-time IntelligentVideo processing and to recorded video searches. The Video Channel Configuration dialog is used to configure event parameters that apply to the video channel itself and not the video processing algorithms. For example, if the source video has a lot of motion, background learning time may need to be increases so the video processing engine picks out static scene elements more accurately.

For detailed IntelligentVideo Event configuration information, refer to the IntelligentVideo User Guide.



Video Channel Configuration listing window

Displays the video channel processing properties and user-configured values. Parameters are sorted into types. Values are modified directly in the listing window. A new value may be entered or selected from the drop-down list. Values that have been modified from the default appear in bold. Click [Explain] to read a detailed description of the selected property.

OK

Accepts the video channel configuration changes and closes the dialog.

Cancel
Rejects the video channel configuration changes and closes the dialog.

Load Configuration
Displays an Open window from which you can select the ".XML" configuration file you want to load.

Save Configuration
Saves the set of video channel configuration parameters for reuse.

Reset to Defaults
Resets all parameter settings to their original default settings.

Show Parameters Only For
Select this check box to display only parameters which are relevant to the selected event. Only events configured for the current channel are available in the drop-down list.

Show Advanced Parameters
Select this check box to view additional parameters used for troubleshooting and diagnostics. The default setting hides the advanced parameters.

Explain
Click this button to read a detailed description of the selected property.

Video Channel Configuration Dialog Procedures

The following procedures can be performed in this dialog.

Configure Video Channel Parameters

Two types of parameters are available: basic and advanced. Parameters are defined per channel and for each event there is a unique set of parameters. You can set parameters by pressing the [Channel Configuration] button in the Event Configuration/Search dialog. By default, only basic parameters display. If you want to set an advanced parameter, click the **Show Advanced Parameters** check box. Advanced parameters should only be set by expert level administrators.

A parameter can be set by entering or selecting a value from the drop-down list in the listing window.

1. Display the Video Configuration dialog. For more information, refer to Open the Video Channel Configuration Dialog on page 1031.
2. It is recommended that you select the **Show Parameters Only For** check box.
3. Select (highlight) a property name.
4. Select or enter the property value.
5. Repeat steps 3 and 4 for each property.
6. Click [Save Configuration] if you would like to be able to load these configurations at another time.

Click [OK].

CHAPTER 51

Matrix Switcher Folder

The folder contains two forms: the Matrix Switcher form and the Matrix Switcher Type form.

The Matrix Switcher folder is displayed by selecting ***Matrix Switcher*** from the ***Video*** menu, or by selecting the Matrix Switchers toolbar button.

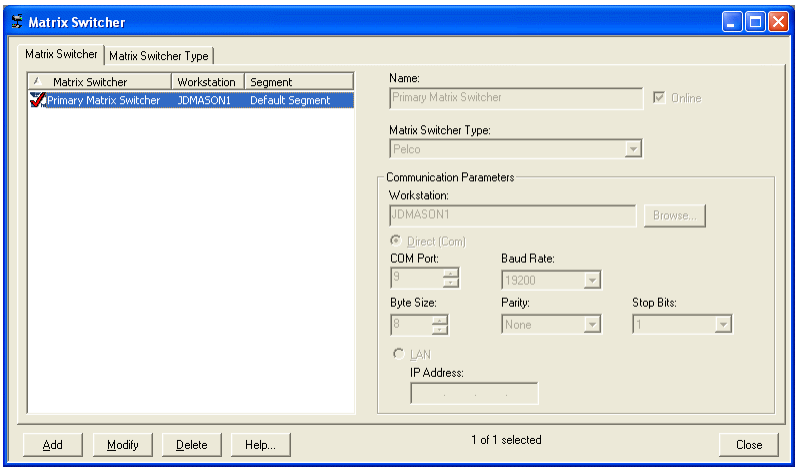
Toolbar Shortcut

Matrix Switcher Overview

Matrix switchers enable Pan, Tilt, and Zoom (PTZ) control for LDVR recorders. Other Lenel video recorders do not require matrix switchers for PTZ control.

The Matrix Switcher folder contains forms with which you can configure real and virtual matrix switchers, as well as matrix switcher types. Real matrix switchers can be used with any OnGuard supported camera or PTZ housing unit. Virtual matrix switchers can be used with Pelco Spectra Dome III cameras. Virtual matrix switchers are configured just like the real matrix switchers.

Matrix Switcher Form



Listing window

Lists currently defined matrix switchers, the name of the workstation connected to each, and the segment each is in (if segmentation is enabled).

Name

Enter a descriptive name for the matrix switcher. This is a “friendly” name assigned to each switcher to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the matrix switcher will be online. Online indicates that the switcher is ready for use, and that the Communication Server will attempt to communicate with it. If the switcher is not marked as online, the Communication Server will not attempt to communicate with it.

Matrix Switcher Type

Select the matrix switcher type from the drop-down list. Choices in the list depend on what types were configured on the Matrix Switcher Type form.

Communication Parameters

Includes the [Browse] button, as well as the **Workstation**, **COM Port**, **Baud Rate**, **Byte Size**, **Parity**, and **Stop Bits** fields.

Workstation

Select the workstation or server to which the matrix switcher is connected in order to transfer information. This is the workstation on which the Communication Server will run. You can either type the name in the field or use the [Browse] button to view a list of available workstations. You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Opens a Browse for Computer window, from which you can click on the name of a workstation.

Direct (COM)

Select this radio button if the workstation will be directly connected to the matrix switcher. If selected, specify the **COM Port**, **Baud Rate**, **Byte Size**, **Parity**, and **Stop Bits**.

COM Port

This field is only available for selection when the **Direct (COM)** radio button is selected. Specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one matrix switcher. Choose a value in the range of 1 through 255.

Baud Rate

This field is only available for selection when the **Direct (COM)** radio button is selected. Select the rate, in bits per second (bps), at which data is transferred via the communication port.

Byte Size

This field is only available for selection when the **Direct (COM)** radio button is selected. Select the byte size of data transferred via the communication port. You can choose a value in the range of 4 through 8.

Parity

This field is only available for selection when the **Direct (COM)** radio button is selected. Select the parity of data transferred via the communication port.

Stop Bits

This field is only available for selection when the **Direct (COM)** radio button is selected. Select the number of stop bits used in data transmission via the communication port.

LAN

Select this radio button if the workstation will communicate with the matrix switcher over a Local Area Network. You must also specify the workstation's **IP Address**.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the matrix switcher, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number.

Add

Adds a matrix switcher record.

Modify

Changes a matrix switcher record.

Delete

Deletes a matrix switcher record.

Help

Displays online help for this form.

Mode

In view mode, indicates the record/selection count (such as "1 of 42 selected"). In modify mode, indicates the current operation, such as "Modify Mode."

Close

Closes the Matrix Switcher folder.

Matrix Switcher Form Procedures

Use the following procedures on this form.

Add a Matrix Switcher (Real and Virtual)

Complete this procedure for either virtual or real matrix switchers.

Note: You may need to add or modify an existing matrix switcher type before adding a matrix switcher. For more information, refer to Add a Matrix Switcher Type on page 1040.

1. From the ***Video*** menu, select ***Matrix Switchers***.
2. On the Matrix Switcher tab, click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this permission group will be assigned to.
   b. Click [OK].
4. In the **Name** field, type a unique, descriptive name for the matrix switcher.
5. Select a type from the **Matrix Switcher Type** drop-down list. If using a virtual matrix switcher select the pre-defined Pelco “D” protocol.
6. If you want to place the matrix switcher online immediately, select the **Online** check box. Typically, you wouldn’t check this box when configuring the system or defining switchers, but instead would wait until you’re ready to put the switcher into service.
7. Complete the Communication Parameters section with respect to the workstation and camera connected to the matrix switcher.
8. Click [OK].
9. Link the camera(s) to the matrix switcher in the Digital Video folder > Camera form > Communication sub-tab. For more information, refer to Camera Form (Communication Sub-tab) on page 940.

Note: For more information regarding virtual matrix switchers refer to the Digital Video Hardware User Guide.

Modify a Matrix Switcher (Real and Virtual)

1. In the listing window, select the matrix switcher entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.
5. Click [OK] to confirm the modification.

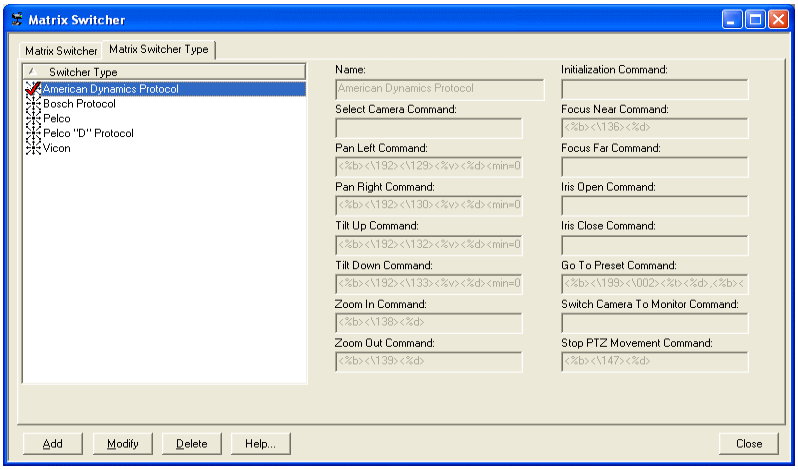
Delete a Matrix Switcher (Real and Virtual)

1. In the listing window, select the matrix switcher entry you wish to delete.
2. Click [Delete].
3. Click [OK].
4. Click [OK] to confirm the deletion.

Matrix Switcher Type Form

The Matrix Switcher Type form contains five pre-defined sets of protocols. Users can add new protocols or customize existing ones.

- **American Dynamics Protocol** - Binary based protocol, used for virtual matrix switchers
- **Bosch Protocol** - Binary based protocol, used for virtual matrix switchers
- **Pelco** - ASCII character based protocol, used for real matrix switchers
- **Vicon** - ASCII character based protocol, used for real matrix switchers
- **Pelco "D" Protocol** - Binary based protocol, used for virtual matrix switchers



Listing window

Lists currently defined matrix switchers types.

Name

Enter a descriptive name for the matrix switcher type. This is a "friendly" name assigned to each matrix switcher type to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Command fields

The input in these fields allow you to control a camera connected to the matrix switcher. OnGuard databases created by the Database Setup application default to commands entered into the command fields for Pelco and Vicon switchers. For more information, refer to Custom Command Grammar for Matrix-based Systems on page 1040.

Add

Adds a matrix switcher type record.

Modify

Changes a matrix switcher type record.

Delete

Deletes a matrix switcher type record.

Help

Displays online help for this form.

Close

Closes the Matrix Switcher folder.

Matrix Switcher Type Form Procedures

Use the following procedures on this form.

Add a Matrix Switcher Type

1. From the ***Video*** menu, select ***Matrix Switchers***.
2. On the Matrix Switcher Type tab, click [Add].
3. In the **Name** field, type a unique, descriptive name for the matrix switcher type.
4. OnGuard databases created by the Database Setup application default to commands entered into the command fields for matrix switchers. For more information, refer to Custom Command Grammar for Matrix-based Systems on page 1040.
5. Click [OK].
6. Now you are ready to add a matrix switcher. For more information, refer to Add a Matrix Switcher (Real and Virtual) on page 1038.

Modify a Matrix Switcher Type

1. In the listing window, select the matrix switcher type entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.
5. Click [OK] to confirm the modification.

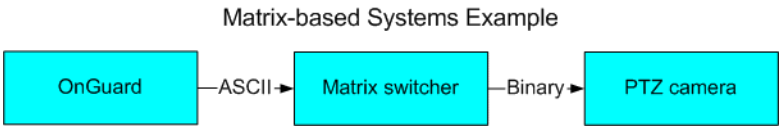
Delete a Matrix Switcher Type

1. In the listing window, select the matrix switcher type entry you wish to delete.
2. Click [Delete].
3. Click [OK].
4. Click [OK] to confirm the deletion.

Custom Command Grammar for Matrix-based Systems

OnGuard includes two default real matrix switcher types: Vicon and Pelco. If you wish to customize the commands, refer to your matrix switcher's documentation and to the ASCII Character Chart. For more information please refer to Appendix F: ASCII Character Chart on page 1429.

Matrix-based systems use ASCII commands. These commands are converted to the correct protocol required by the camera at the matrix switcher, and are then used to control PTZ cameras. On a very simple level, this is the path a command takes when a matrix-based system is used with OnGuard to control a PTZ camera:



Unfortunately, not all matrix switcher protocols send ASCII only commands. Many protocols need to send carriage returns, escape sequences, non-printable characters, or line feeds at the end of a control sequence. Below is a list of variables used within the commands to allow the commands to control the camera at the proper speed, operate the proper preset, etc. from within Alarm Monitoring:

<%c>	Escape sequence representing the replacement of the <%c> with the channel number of the camera the command should act on.
<%m>	Escape sequence representing the replacement of the <%m> with the monitor number (used in the switch camera x to monitor y command).
<%p>	Escape sequence representing the replacement of the <%p> with the preset number to go to.
<%s>	Escape sequence representing the replacement of the <%s> with the speed number.
<\nnn>	<\nnn> is an ASCII decimal representation of an ASCII character code. During transmission, this is converted to an ASCII character. The “nnn” should be in the form of “0” - “255.” For example, <\013> is converted to a carriage return.
All other characters	All other characters are to be treated as literal characters and sent as is out the RS-232 COM port.
<min=nn>	Lower range for speed if command takes a speed parameter. Note that this value is used internally by the system and is not sent down as part of the command. If the switcher you are connecting to supports a speed range from 1 to 100, this parameter is not required. This command only applies to PTZ controls. It does not apply for Iris or Focus commands.
<max=nn>	Upper range for speed if command takes a speed parameter. Note that this value is used internally by the system and is not sent down as part of the command. If the switcher you are connecting to supports a speed range from 1 to 100, this parameter is not required. This command only applies to PTZ controls. It does not apply for Iris or Focus commands.

Examples:

The command to tell a Pelco switcher to pan camera 1 left at a speed of 10, would be:

<%c>#a<%s>La<min=1><max=64>

The min and max values are added because the Pelco matrix switcher only allows speeds in the range of 1-64. The video player will send speeds in a percentage from 1-100, based on the distance of the mouse from the center when the command was sent. The Communication Server will interpolate the percentage into the allowable range.

Note: Some matrix switchers require a mandatory character length for their channel, monitor, preset, and speed numbers. In these cases, commands are sent to the switcher with the

total number of mandatory characters. When the number of characters in the channel, monitor, preset, or speed number does not amount to the mandatory character length (represented by “n” in the escape sequence), the number is padded with one or more zeros. When required, escape sequences can be padded with up to 10 pad characters (zeros).

If “n” represents the number “2” in the escape sequence <%sn>, then 2 is the total number of characters that are sent to the matrix switcher. Therefore, if the speed number is 1-9, then that number is preceded (padded) by a “0”.

- When the speed number is 4: <%s2> = 04
- When the speed number is 12: <%s2> = 12

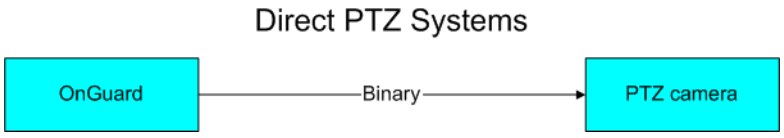
If “n” represents the number “3” in the escape sequence <%mn>, then 3 is the total number of characters that are sent to the matrix switcher. Therefore, monitor numbers 1-9 are preceded (padded) by “00”. Monitor numbers 10-99 are preceded (padded) by “0”.

- When the monitor number is 6: <%m3> = 006
- When the monitor number is 58: <%m3> = 058
- When the monitor number is 105: <%m3> = 105

Custom Command Grammar for Direct PTZ Systems

Note: Custom command programming for direct PTZ systems is very complex and may not work with all devices. Configuration of these systems is not recommended without the involvement of Lenel’s software engineers.

Direct PTZ systems do not use an actual physical matrix switcher. Instead, binary commands may be used to directly control a PTZ camera. On a very simple level, this is the path a command takes when a direct PTZ system is used with OnGuard to control a PTZ camera:



“D” Protocol

“D” protocol is used between matrix switching systems and receivers (cameras). The default Pelco “D” Protocol matrix switcher type uses this protocol.

“D” Protocol Message Format

The format for a message is:

Byte 1	Synch Byte
Byte 2	Address
Byte 3	Command 1
Byte 4	Command 2
Byte 5	Data 1

Byte 6	Data 2
Byte 7	Check Sum

All values below are shown in hexadecimal (base 16).

The synchronization byte is always $FF.

The address is the logical address of the receiver/driver being controlled.

The check sum is the 8 bit (modulo 256) sum of the payload bytes (bytes 2 through 6) in the message. This is generated by the OnGuard system.

"D" Protocol Standard Command Set

Command 1 and 2 are as follows:

Byte	Command 1	Command 2
Byte 7	Sense	Focus Far
Byte 6	Reserved	Zoom Wide
Byte 5	Reserved	Zoom Tele
Byte 4	Auto/Manual Scan	Down
Byte 3	Camera On/Off	Up
Byte 2	Iris Close	Left
Byte 1	Iris Open	Right
Byte 0	Focus Near	Always 0

The sense bit (command 1 bit 7) indicates the meaning of bits 4 and 3. If the sense bit is on, and bits 4 and 3 are on, the command will enable auto-scan and turn the camera on. If the sense bit is off and bits 4 and 3 are on the command will enable manual scan and turn the camera off. Of course, if either bit 4 or bit 3 are off then no action will be taken for those features.

The reserved bits (6 and 5) should be set to 0.

Word 5 contains the pan speed. Pan speed is in the range $00 (stop) to $3F (high speed) and $FF for "turbo" speed. Turbo speed is the maximum speed the device can obtain and is considered separately because it is not generally a smooth step from high speed to turbo. That is, going from one speed to the next usually looks smooth and will provide for smooth motion with the exception of going into and out of turbo speed.

Word 6 contains the tilt speed. Tilt speed is in the range $00 (stop) to $3F (maximum speed).

Word 7 is the check sum. The check sum is the sum of bytes (excluding the synchronization byte) modulo 256.

Matrix Switcher Variable Designations

Control Variable	Standard (Hardware) Commands (Vicon shown)	ASCII Variables	Protocol D commands	Binary Variables
Camera		%c		%b
Initialization	<\1>A001<\13>			
Pan left	<\1>B<%c><\13><\1>I<%s><\13><min=1><max=100>		<\255><%b><\000><\004><%v><\000><%x><min=0><max=63>	
Pan right	<\1>B<%c><\13><\1>J<%s><\13><min=1><max=100>		<\255><%b><\000><\002><%v><\000><%x><min=0><max=63>	
Tilt up	<\1>B<%c><\13><\1>M<%s><\13><min=1><max=100>		<\255><%b><\000><\008><\000><%v><%x><min=0><max=63>	
Tilt down	<\1>B<%c><\13><\1>L<%s><\13><min=1><max=100>		<\255><%b><\000><\016><\000><%v><%x><min=0><max=63>	
Zoom in	<\1>B<%c><\13><\1>O<\13>		<\255><%b><\000><\032><\000><\000><%x>	
Zoom out	<\1>B<%c><\13><\1>N<\13>		<\255><%b><\000><\064><\000><\000><%x>	
Focus near	<\1>B<%c><\13><\1>P<\13>		<\255><%b><\001><\000><\000><\000><%x>	
Focus far	<\1>B<%c><\13><\1>Q<\13>		<\255><%b><\000><\128><\000><\000><%x>	
Iris open	<\1>B<%c><\13><\1>S<\13>		<\255><%b><\002><\000><\000><\000><%x>	
Iris close	<\1>B<%c><\13><\1>R<\13>		<\255><%b><\004><\000><\000><\000><%x>	
Preset	<\1>B<%c><\13><\1>G<%p><\13>	%p	<\255><%b><\000><\007><\000><%t><%x>	%t
Stop PTZ	<\1>B<%c><\13><\1><\13>		<\255><%b><\000><\000><\000><\000><%x>	
Speed		%s		%v
Switch Camera to Monitor	<\1>A<%m><\13><\1>B<%c><\13>	%m	N/A	
Checksum for Protocol D				%x

ASCII Protocol Example: Pan Left

Select camera	<\1>B<%c><\13>
Pan left (I)	<\1>I<%s><\13>
at speed (1-100)	<min=1><max=100>

Binary (“D” Protocol) Example: Pan Left

Sync byte	<\255>
Logical cam address	<%b>
Command 1 (dec)	<\000>
Command 2 (dec)	<\004>
Data 1	<%v>
Data 2	<\000>
Check sum	<%x>
at speed (0-63)	<min=0><max=63>

For more information, refer to the Pelco “D” Protocol Manual.

Additional Hardware

CHAPTER 52

Fire Panels Folder

The Fire Panels folder contains forms with which you can provide an interface to your fire alarm system.

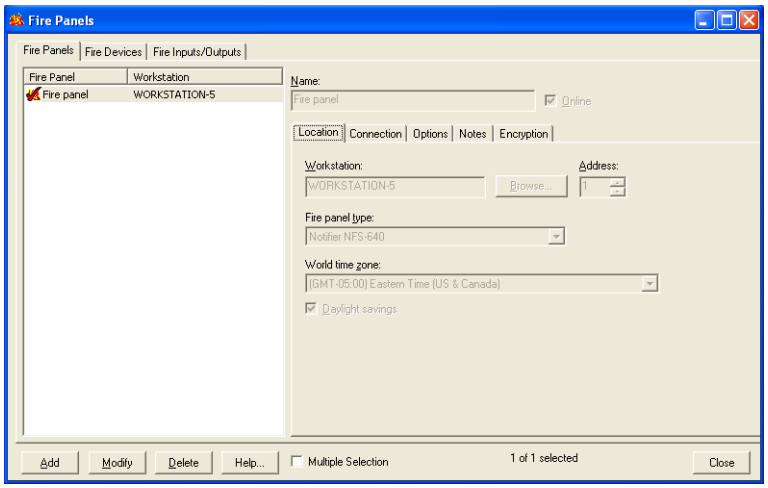
The folder contains three forms, the Fire Panels form, the Fire Devices form, and the Fire Inputs/ Outputs form.

The Fire Panels folder is displayed by selecting ***Fire Panels*** from the ***Additional Hardware*** menu, or by selecting the Fire Panels toolbar button.

Toolbar Shortcut

IMPORTANT: Because of hardware limitations, the Notifier NFS-640 panel always appears to be online in the Alarm Monitoring application. Therefore the panel should physically be checked to verify that it's actually online.

Fire Panels Form (Location Sub-tab)



Listing window

Lists currently defined fire panels and the name of the workstation that is connected to each. An icon precedes each entry.

Name

Enter a name for the fire panel. Each name must be unique and can contain no more than 32 characters. This is a “friendly” name assigned to each panel to make it easy to identify in the software.

Because of hardware limitations, the Notifier NFS-640 panel always appears to be online in the Alarm Monitoring application. Therefore the panel should physically be checked to verify that it’s actually online.

Online

If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Add

Used to add a fire panel entry.

Modify

Used to change a fire panel entry.

Delete

Used to remove a fire panel entry.

Help

Displays pertinent help information on screen.

Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously.

Close

Closes the Fire Panels folder.

Workstation

Select the name of the computer to which the fire panel is connected. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer from which you can click on the name of a workstation to highlight the entry. Click on the [OK] button to then enter the workstation name in the **Workstation** field on this form.

Address

Select the number that matches the address of the fire panel. Possible values are in the range of 1 through 255. The fire panel address is set using the CSGM configuration tool. By default, the address is 1 if you have a one-panel system. If you have multiple panels, you must use CSGM to set the address for each panel. You must also set this address on the NIM-1R board.

Fire panel type

Contains a list of fire panel types that are valid for the installed software license.

World time zone

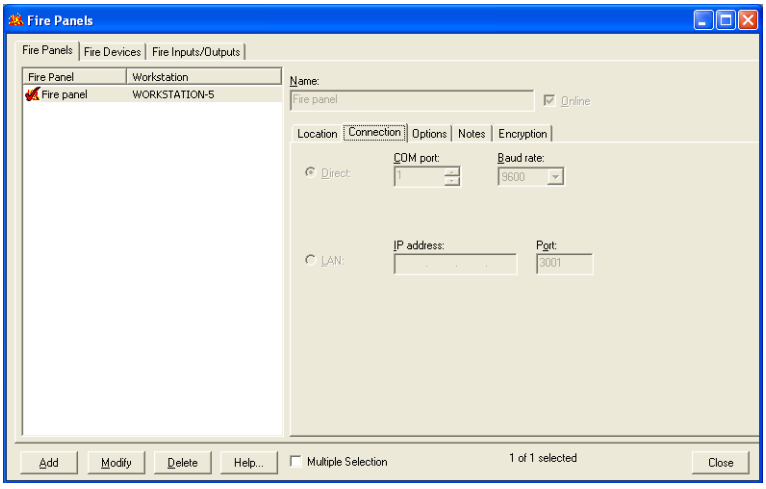
Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Fire Panels Form (Connection Sub-tab)



Connection Sub-tab

Direct

Select this radio button if the workstation will be directly connected to the fire panel. You must also specify the **COM port** and **Baud rate**.

COM port

Enabled only when the **Direct** radio button is selected. Choose the number of the port (on the serial expansion unit or the back of the workstation or server) that will be used for communication with the panel. Choose a value in the range of 1 through 256.

Baud rate

This is the speed (in bits per second) at which information is transferred between the workstation and the fire panel.

LAN

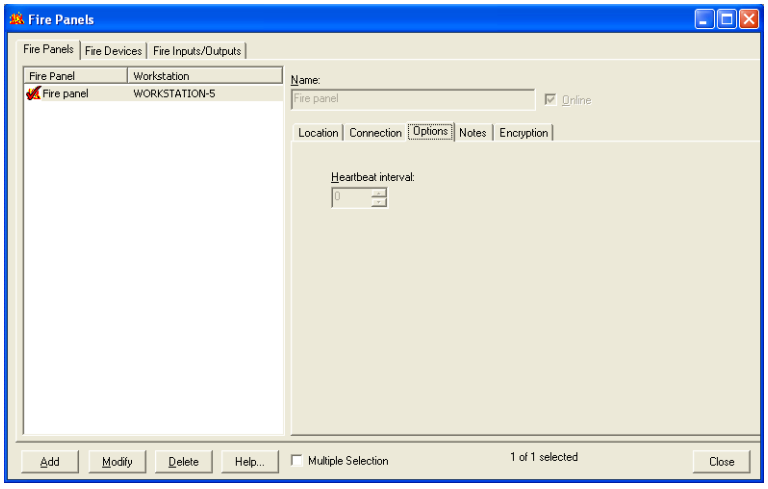
Select this radio button if the workstation will communicate with the fire panel over a Local Area Network. You must also specify the workstation's **IP Address**.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the fire panel, as provided by your LAN Network Administrator.

An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number.

Fire Panels Form (Options Sub-tab)



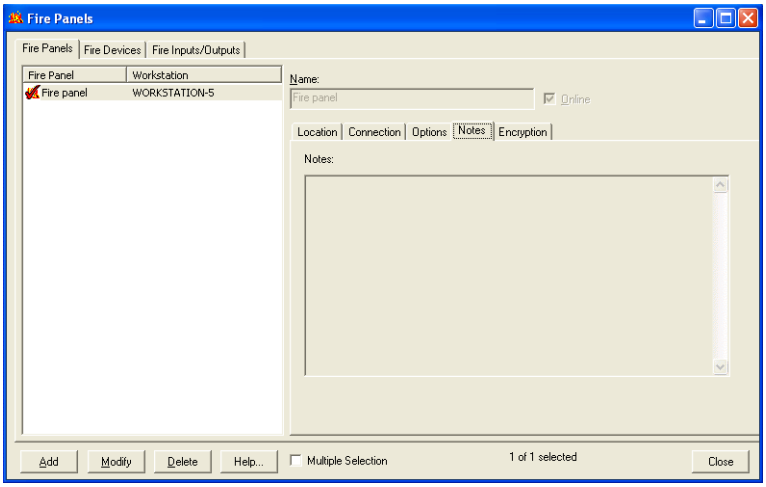
Heartbeat interval

This field is enabled if you have selected "Notifier AM2020" from the **Fire panel type** drop-down list on the Location sub-tab, or if you've selected the "Tateco" fire panel using selected ESPA protocol. The default heartbeat interval for the Notifier AM2020 is 90 seconds, and the default heartbeat interval for the Tateco ESPA is 0 seconds.

Indicates the heartbeat interval of the selected panel. The heartbeat interval is the time (in seconds) between signals that determine a panel's online or offline status. By default, a signal is

sent out approximately once every minute. This means that a panel may be offline for a full minute before the system is notified. If you increase the interval between signals, the heartbeat interval, you are increasing the time that a panel may be offline before the system is notified.

Fire Panels Form (Notes Sub-tab)

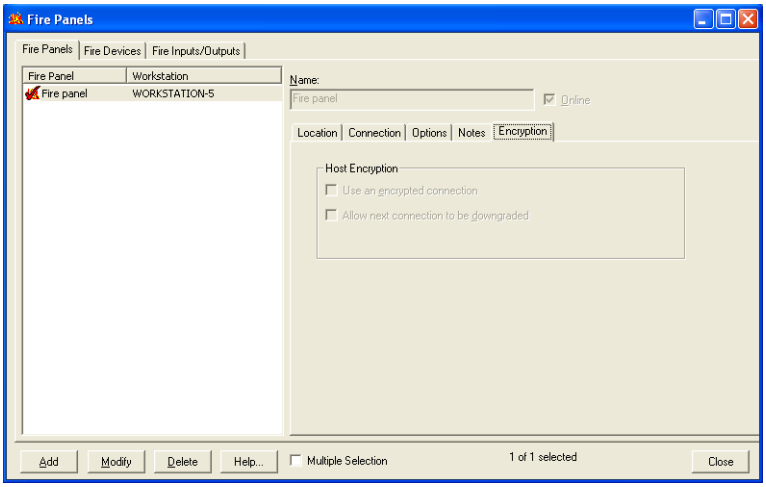


Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

Fire Panels Form (Encryption Sub-tab)

Note: Configuration on this tab will be disabled unless the panel is configured for a LAN connection type on the Connection sub-tab.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key and then by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible. This check box displays only if the controller exists in an automatic key management system/segment.

Fire Panels Form Procedures

Use the following procedures on this form.

Add a Fire Panel

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. Click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this fire panel will be assigned to.
   b. Click [OK].
4. In the **Name** field, type a unique, descriptive name for the fire panel.
5. Select the **Online** check box if you want the panel to be online.
6. On the Location sub-tab:
   a. In the **Workstation** field enter the name of the workstation the fire panel will be connected to. It's best to select the workstation using [Browse]. In the Browse for Computer window, select the name of the workstation, then click [OK].

Note: You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

   b. Select the number that matches the **Address** of the fire panel. Possible values are in the range of 1 through 255.

Note: The fire panel address is set using the CSGM configuration tool. By default, the address is 1 if you have a one-panel system. If you have multiple panels, you must use CSGM to set the address for each panel. You must also set this address on the NIM-1R board.

   c. Select the **Fire panel type**.
   d. Select the world time zone from the **World time zone** drop-down list.
   e. Select whether **Daylight savings** is used or not.
7. On the Connection sub-tab:
   a. If the workstation will communicate with the fire panel directly, select the **Direct** radio button and specify the **COM port** and **Baud rate**.

   b. If the workstation will communicate with the fire panel over a LAN, select the **LAN** radio button and specify the **IP address**.

8. If you selected "Notifier AM2020" or a "Tateco" fire panel from the **Fire panel type** drop-down list on the Location sub-tab, select the Options sub-tab to determine the panel's **Heartbeat interval**. The heartbeat interval is the time (in seconds) between signals that determine a panel's online or offline status. By default, a signal is sent out approximately once every minute. This means that a panel may be offline for a full minute before the system is notified. If you increase the interval between signals, the heartbeat interval, you are increasing the time that a panel may be offline before the system is notified.
9. Click [OK].

Modify a Fire Panel

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. In the listing window, select the fire panel entry you wish to change.
3. Click [Modify].
4. Make the changes you want to the fields. Changes can be made on any sub-tab.
5. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Fire Panel

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. In the listing window, select the fire panel entry you wish to delete.
3. Click [Delete].
4. Click [OK].

Enable a Fire Panel for Encryption

The encryption modify/export permission is required to complete this procedure. Also, encryption must be enabled and the proper encryption key configured in the communication device before enabling the panel for encryption.

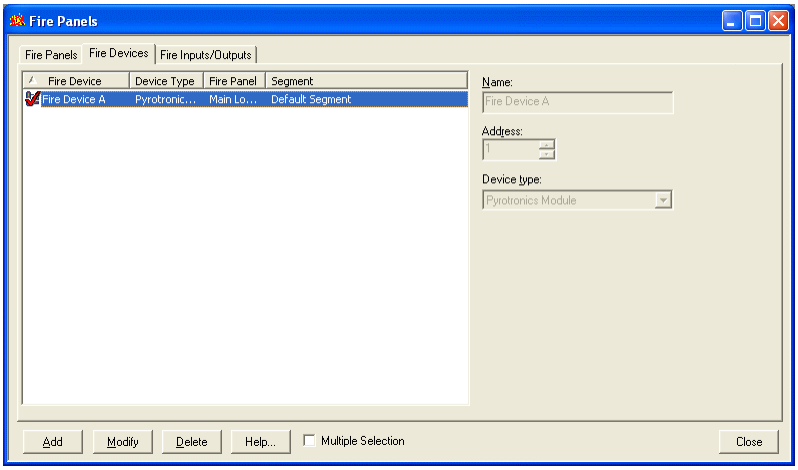
1. From the ***Additional Hardware*** menu, select ***Fire Panels***.
2. On the Fire Panel form, click the Encryption sub-tab.
3. In the listing window, select the Fire Panel entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Enter Notes for a Panel

1. In the listing window, select the entry you want to edit.
2. Click [Modify].

3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Fire Devices Form



Listing window

In view mode, displays currently defined fire devices. In add or modify mode, displays currently defined fire panels.

Name

In add or modify mode, enter a name for the fire device. Each name must be unique and can contain no more than 32 characters. This is a “friendly” name assigned to each device to make it easy to identify in the software.

Address

In add or modify mode, select the number that matches the address of the fire device. Possible values are in the range of 1 through 255.

Device type

In add or modify mode, select the type of fire device. Choices in the drop-down list depend on which fire panel the selected fire device is configured with.

Add

Used to add a fire device entry.

Modify

Used to change a fire device entry.

Delete

Used to remove a fire device entry.

Help

Displays online help for this form.

Multiple Selection
If selected, more than one entry in the listing window can be checked simultaneously.

Close
Closes the Fire Panels folder.

Fire Devices Form Procedures

Use the following procedures on this form.

Add a Fire Device

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. Select the Fire Devices tab.
3. Click [Add].
4. From the listing window, select the name of the panel that you want to configure this device with.
5. In the **Name** field, type a unique, descriptive name for the fire device.
6. Select the number that matches the **Address** of the fire device. Possible values depend on the type of panel used.
7. Select the **Device type**. Choices in the drop-down list depend on which fire panel this fire device is configured with.
8. Click [OK].

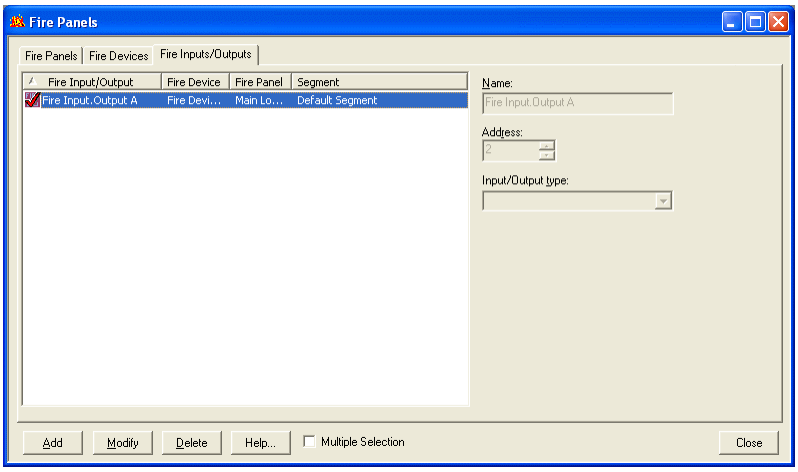
Modify a Fire Device

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. Select the Fire Devices tab.
3. In the listing window, select the fire device entry you wish to change.
4. Click [Modify].
5. Make the changes you want to the fields.
6. Click [OK].
7. A Confirm Record Modify message will be displayed. Click [OK] to complete the modification.

Delete a Fire Device

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. Select the Fire Devices tab.
3. In the listing window, select the fire device entry you wish to delete.
4. Click [Delete].
5. Click [OK].
6. A Confirm Record Delete message will be displayed. Click [OK] to complete the deletion.

Fire Inputs/Outputs Form



Listing window

In view mode, displays currently defined fire inputs/outputs. In add or modify mode, displays currently defined fire devices.

Name

In add or modify mode, enter a name for the fire input/output. Each name must be unique and can contain no more than 32 characters. This is a “friendly” name assigned to each fire input/output to make it easy to identify in the software.

Address

In add or modify mode, select the number that matches the address of the fire input/output. Possible values are in the range of 1 through 255.

Inputs/Outputs type

Only used for a Loop on a Notifier NFS-64, and Notifier AM2020 fire panel. Is used to specify what type of input is being added. This is necessary because the Notifier NFS-640, and AM2020 allows different types of inputs to be configured with the same address. Notifier AM2020 Loop functionality is only available in OnGuard build 5.11.xxx and up. This was also added as a hot fix for build 5.10.423.

Add

Used to add a fire inputs/outputs entry.

Modify

Used to change a fire inputs/outputs entry.

Delete

Used to remove a fire inputs/outputs entry.

Help

Displays online help for this form.

Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously.

Close

Closes the Fire Panels folder.

Fire Inputs/Outputs Form Procedures

Use the following procedures on this form.

Add a Fire Input/Output

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. Select the Fire Inputs/Outputs tab.
3. Click [Add].
4. From the listing window, select the name of the device that you want to configure this input/output with.
5. In the **Name** field, type a unique, descriptive name for the fire input/output.
6. Select the number that matches the **Address** of the fire input/output. Possible values are in the range of 1 through 255.
7. Click [OK].

Modify a Fire Input/Output

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. Select the Fire Inputs/Outputs tab.
3. In the listing window, select the fire input/output entry you wish to change.
4. Click [Modify].
5. Make the changes you want to the fields.
6. Click [OK].
7. A Confirm Record Modify message will be displayed. Click [OK] to complete the modification.

Delete a Fire Input/Output

1. From the ***Additional Hardware*** menu, select ***Fire Panels***. The Fire Panels folder opens.
2. Select the Fire Inputs/Outputs tab.
3. In the listing window, select the fire input/output entry you wish to delete.
4. Click [Delete].
5. Click [OK].
6. A Confirm Record Delete message will be displayed. Click [OK] to complete the deletion.

CHAPTER 53

Intercom Devices Folder

The Intercom Devices folder contains forms with which you can:

- Configure OnGuard to use exchanges for intercom communication
- Configure OnGuard to use intercom stations
- Configure OnGuard to recognize intercom functions
- Link a cardholder field to an intercom station (using the Automatic Lookup form)

The folder contains three forms: the Intercom Devices, the Intercom Stations form, and the Intercom Functions form.

The Intercom Devices folder is displayed by selecting ***Intercom Devices*** from the ***Additional Hardware*** menu, or by selecting the Intercom toolbar button.

Toolbar Shortcut

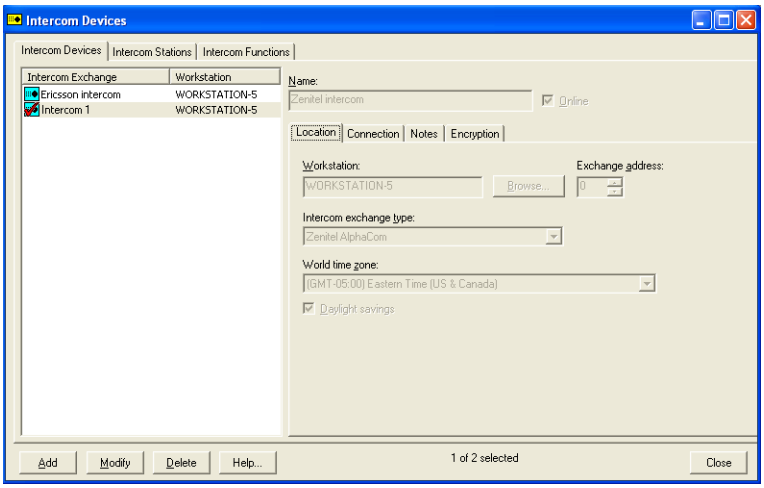
Intercom Communication

OnGuard supports the Ericsson MD110 and generic intercom systems in addition to supporting other intercom systems through the OnGuard SDK. Intercom system hardware consists of stations and exchanges. The *station* is the actual unit a person uses to make calls. Each station is connected to an exchange unit, which is referred to as an *intercom exchange*.

Ericsson MD110 Intercom System

OnGuard communicates with the Ericsson MD110 system using the Application Link client DLL. Therefore, the Application Link client DLL must be installed on the machine running the OnGuard Communication Server.

Intercom Devices Form (Location Sub-tab)



Intercom exchange listing window

Lists all currently defined intercom exchanges. Each entry includes the name of the exchange, the workstation the exchange is attached to, and the segment it is in. (The Segment column appears only if segmentation is enabled on your system.)

Name

Indicates the name of the main exchange.

Online

If selected, the exchange is online. If not selected, the exchange is offline.

Add

Used to add an intercom exchange record.

Modify

Used to change an intercom exchange record.

Delete

Used to remove an intercom exchange record.

Help

Displays online assistance for this form.

Close

Closes the Intercom Devices folder.

Workstation

Identifies the workstation the exchange is attached to. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/ configured.)

Browse

Opens a Browse for Computer window, from which you can select a workstation.

Exchange address
Identifies the intercom.

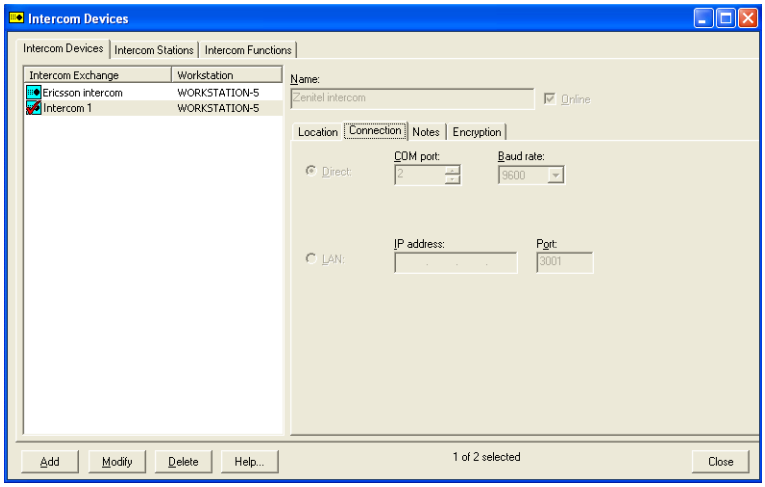
Intercom exchange type
Displays a list of intercom exchange types.

World time zone
Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings
Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Intercom Devices Form (Connection Sub-tab)



Direct
Select this radio button if the workstation will communicate with the intercom exchange over a direct serial connection.

COM port
If you selected the **Direct** radio button, specify the serial port the intercom exchange is attached to (along with the baud rate).

Baud rate
If you selected the Direct radio button, enter the speed (in bits per second) at which information is transferred between the workstation and the intercom exchange.

LAN

Select the **LAN** radio button if the workstation will communicate with the intercom exchange over a Local Area Network.

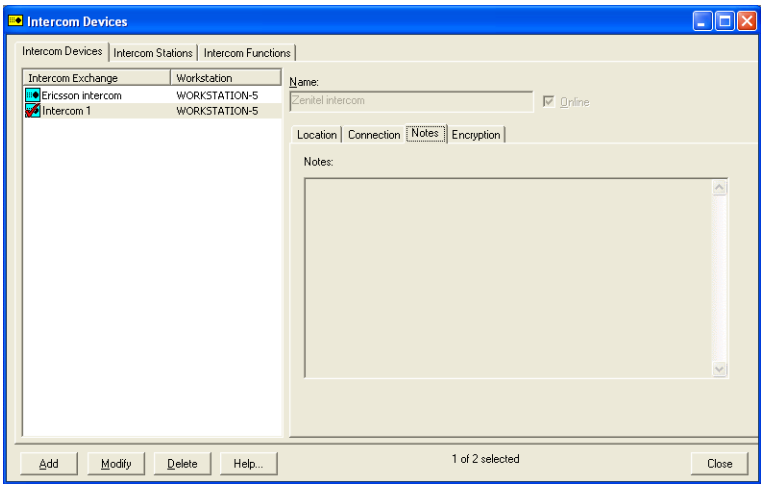
IP address

If you selected the **LAN** radio button, enter the Internet Protocol (TCP/IP) address for the intercom exchange, as provided by your LAN Network Administrator.

Port

This field applies to Ericsson MD110 intercoms only. Enter the port the Application Link client DLL uses (along with the IP address) to communicate with the Ericsson MD110. Port values range from 1-65535.

Intercom Devices Form (Notes Sub-tab)

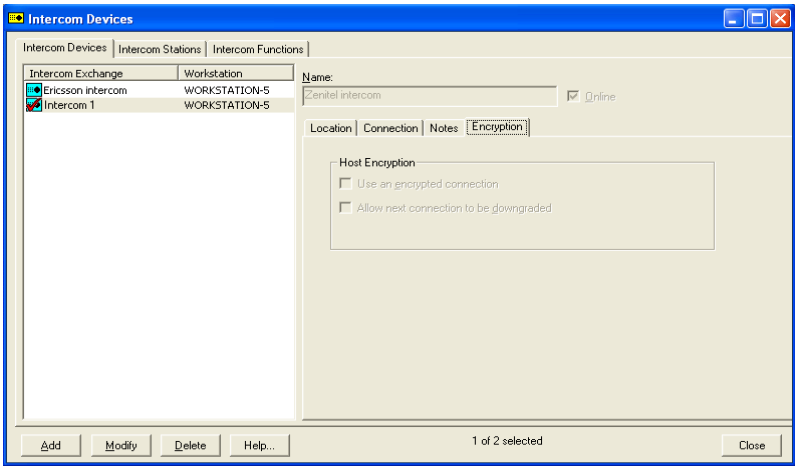


Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

Intercom Devices Form (Encryption Sub-tab)

Note: Configuration on this tab will be disabled unless the panel is configured for a LAN connection type on the Connection sub-tab.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key and then by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible. This check box displays only if the controller exists in an automatic key management system/segment.

Intercom Devices Form Procedures

Use the following procedures on this form.

Add an Intercom Exchange

1. From the ***Additional Hardware*** menu, select ***Intercom Devices***.
2. On the Intercom Devices form, click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this intercom exchange will be assigned to.
   b. Click [OK].
4. In the **Name** field, type a unique, descriptive name for the exchange.
5. Select the **Online** check box if the exchange will be online, or de-select the check box if the exchange will be offline.
6. On the Location sub-tab:
   a. Enter the name of the workstation the exchange will connect to.

   b. Enter the intercom exchange address. This field applies to generic and the OnGuard SDK intercom exchanges.
   c. Select the type of intercom exchange from the drop-down list.
   d. Select the world time zone from the **World time zone** drop-down list.
   e. Select whether **Daylight savings** is used or not.
7. On the Connection sub-tab, select the method used to communicate with the exchange. Note that only network connections are allowed when adding an Ericsson MD110 exchange.
   a. Select the **Direct** radio button if communication with the exchange will be through a direct serial connection to the specified workstation. You must also specify the workstation's COM port and baud rate.
   b. Select the **LAN** radio button if communication with the exchange will be over a Local Area Network. You must also specify the workstation's IP address, and for Ericsson MD110 exchanges you must also specify the port.
8. Click [OK]. A record for the exchange will be added to the listing window.

Modify an Intercom Exchange

1. From the ***Additional Hardware*** menu, select ***Intercom Devices***.
2. On the Intercom Devices form, select the intercom exchange you wish to change.
3. Click [Modify].
4. Make the changes you want to the fields. Changes can be made on any sub-tab.
5. Click [OK].
6. The Confirm Record Modify window opens. Click [OK] to complete the changes, or [Cancel] to abandon your changes.

Delete an Intercom Exchange

1. From the ***Additional Hardware*** menu, select ***Intercom Devices***.
2. On the Intercom Devices form, select the intercom exchange you wish to delete.
3. Click [Delete].
4. Click [OK].
5. Click [OK] when prompted to proceed with the deletion, or [Cancel] to abandon the deletion.

Enable an Intercom Exchange for Encryption

The encryption modify/export permission is required to complete this procedure. Also, encryption must be enabled and the proper encryption key configured in the communication device before enabling the panel for encryption.

1. From the ***Additional Hardware*** menu, select ***Intercom Devices***.
2. On the Intercom Exchange form, click the Encryption sub-tab.
3. In the listing window, select the Intercom Exchange entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].

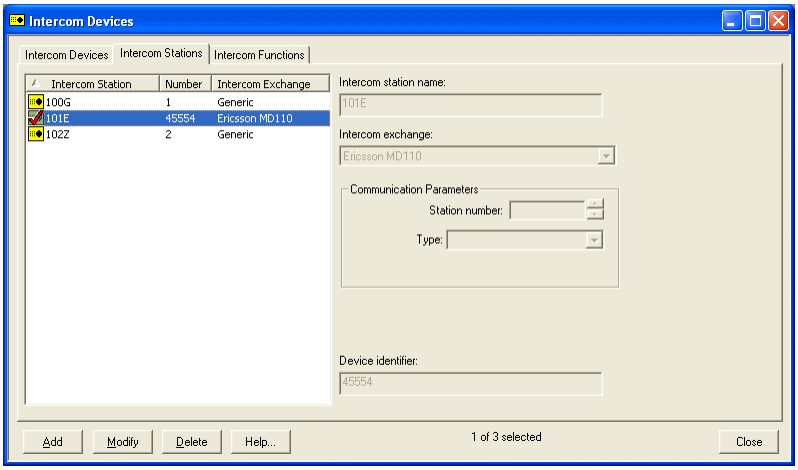
8. Acknowledge any messages that display.

Enter Notes for an Intercom Exchange

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Intercom Stations Form

This form is used to configure communication parameters for intercom stations.



Intercom station listing window

Lists all currently defined intercom stations. Each entry includes the name of the intercom station, its number, the intercom exchange it is attached to, and the segment it is in. (The Segment column appears only if segmentation is enabled on your system.)

Intercom station name

Specify the name of the intercom station.

Intercom exchange

Select the exchange the intercom station is attached to.

Station number

Enter the number individuals should use when calling this station. The combination of intercom exchange and station number must be unique. For most intercom stations the station number cannot be greater than 32766. If you can enter a station number greater than 32766 however, an error message displays “Missing or Invalid Address” when you attempt to add the record.

Cell number

This field displays if you previously linked any cardholder field to a type of intercom panel in the Automatic Lookup form in the Cardholder Options folder. For more information, refer to

Automatic Lookup Form on page 441. The **Cell number** field may not display until you select the intercom exchange.

Type

Assign Avaya (an OnGuard SDK exchange) one of the following types: Analog, IP, or Advanced IP. This field will not be available for most exchanges.

Device identifier

This field applies only to Ericsson MD110 intercom systems. The device identifier consists of numbers (0-9) and can be from 2 to 5 digits long. There is a limit of 8000 devices per Ericsson MD110 intercom exchange. This limit should be taken into consideration when installing the intercom system. For more information, refer to the Ericsson MD1100 manual.

Add

Used to add an intercom station record.

Modify

Used to change an intercom station record.

Delete

Used to remove an intercom station record.

Help

Displays online assistance for this form.

Mode

In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”

Close

Closes the Intercom Devices folder.

Intercom Stations Form Procedures

Use the following procedures on this form.

Add an Intercom Station

You may not add an intercom station until the exchange it is associated with has been defined on the Intercom Devices form.

1. Select ***Intercom Devices*** from the ***Additional Hardware*** menu. The Intercom Devices folder opens.
2. On the Intercom Stations form, click [Add].
3. In the **Intercom station name** field, type a unique, descriptive name for this intercom station.
4. Select the intercom exchange from the drop-down list.

Note: If the intercom exchange you select has a cardholder field associated with it, an additional field, **Cell number**, displays on the Intercom Stations form. For more information, refer to Automatic Lookup Form on page 441.

5. In the Communication Parameters section, specify the intercom station number. The combination of the intercom exchange and the station number must be unique. The station number cannot be greater than 32766.
6. If you are linking a cell number to an intercom station, enter the cell number.
7. Ericsson MD110 stations only - enter the device identifier.

Note: There is a limit of 8000 devices per Ericsson MD110 intercom exchange. This limit should be considered when installing the intercom system. For more information, refer to the Ericsson MD1100 manual.

8. Click [OK]. An intercom station record will be added to the listing window.

Modify an Intercom Station

1. Select ***Intercom Devices*** from the ***Additional Hardware*** menu. The Intercom Devices folder opens.
2. On the Intercom Stations form, select the intercom station record you wish to change.
3. Click [Modify].
4. Make the changes you want to the fields. You may change the **Intercom station name** and **Station number** fields, but you cannot change the **Intercom exchange** field.
5. Click [OK] to proceed with the deletion, or [Cancel] to abandon the deletion.

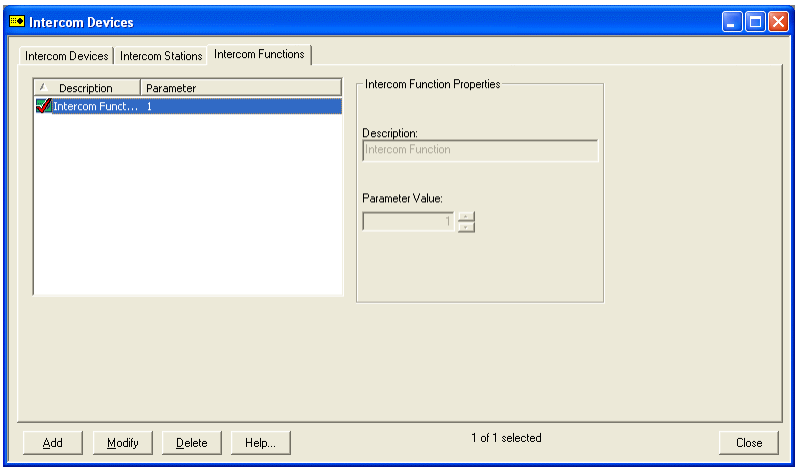
Delete an Intercom Station

1. Select ***Intercom Devices*** from the ***Additional Hardware*** menu. The Intercom Devices folder opens.
2. On the Intercom Stations form, select the intercom station record you wish to delete.
3. Click [Delete].
4. Click [OK].

Intercom Functions Form

The Intercom Functions form is used to:

- Configure intercom functions for Generic intercom systems only. Intercom functions are not supported with Ericsson MD110 systems.
- Change the description and/or parameter values given to intercom functions that are added by the Communication Server.
  If the Communication Server receives an event that includes a parameter value not found in the database, the Communication Server will add an entry into the database, including the parameter value and a default description. Therefore, the listing window of the Intercom Functions form may display records that you did not enter because the Communication Server can add entries.



Intercom functions listing window

Lists all currently defined intercom functions. Each entry includes a description and parameter number.

Description

The description given to the intercom function event with a certain parameter value.

Parameter Value

The parameter value that is returned in the event.

Add

Used to add an intercom function record.

Modify

Used to change an intercom function record.

Delete

Used to delete an intercom function record.

Help

Displays online assistance for this form.

Close

Closes the Intercom Devices folder.

Intercom Functions Overview

Intercom functions are defined in OnGuard so that additional information can display with events in Alarm Monitoring.

Functions are activated at an intercom station, and may be programmed by referring to the documentation included with the manufacturer of the intercom systems.

When a function is activated at a intercom station, an event is generated. The event travels from the intercom station to the exchange, and finally arrives at the Communication Server. Each function has a unique parameter value that is sent in the event. This parameter value is used by the Communication Server to determine which function was activated at the intercom station. You may set the parameter value for a specific function in the **Parameter Value** field on the Intercom Functions form.

Intercom Functions Form Procedures

Use the following procedures on this form.

Add an Intercom Function

1. Select ***Intercom Devices*** from the ***Additional Hardware*** menu. The Intercom Devices folder opens.
2. On the Intercom Functions form, click [Add].
3. In the **Description** field, type a description for this intercom function. (The description does not need to be unique.)
4. Use the spin buttons to choose a parameter value.

Note: Each parameter value must be unique, when you configure multiple functions. When a function generates an event, the event and the parameter value of the function are sent to the Communication Server. The Communication Server uses the parameter value to determine which function triggered the event.

5. Click [OK]. An intercom function record will be added to the listing window.

Modify an Intercom Function

1. Select ***Intercom Devices*** from the ***Additional Hardware*** menu. The Intercom Devices folder opens.
2. On the Intercom Functions form, select the intercom function you wish to change.
3. Click [Modify].
4. Make the changes you want to the **Description** field and/or the **Parameter Value** field.
5. Click [OK].
6. A warning message is displayed that says your change may cause some historical information to be lost. Click [OK] to proceed with the modification, or [Cancel] to not make the modification.

Delete an Intercom Function

1. Select ***Intercom Devices*** from the ***Additional Hardware*** menu. The Intercom Devices folder opens.
2. On the Intercom Functions form, select the intercom function you wish to delete.
3. Click [Delete].
4. Click [OK].
5. A warning message is displayed that says your deletion may cause some historical information to be lost. Click [OK] to proceed with the deletion, or [Cancel] to not make the deletion.

CHAPTER 54

Personal Safety Devices Folder

The Personal Safety Devices folder contains forms with which you can:

- Configure personal safety panels, including Visonic SpiderAlert SLC-5s, for use with OnGuard software
- Configure transmitters that communicate with personal safety receivers to be recognized by OnGuard software
- Configure transmitters that communicate with personal safety receivers to be recognized by OnGuard software
- Modify or delete entries for transmitters
- Configure a transmitter to be masked all the time
- Configure a transmitter to be assigned to be masked during a particular timezone
- Assign a transmitter to an asset or a cardholder
- Modify the name of a transmitter input
- Assign transmitter inputs to assets
- Configure panels so that commands can be sent to the hardware

The folder contains four forms, the Personal Safety Panels form, Transmitters form, Transmitter Inputs form, and the Device Configuration form.

The Personal Safety Devices folder is displayed by selecting ***Personal Safety Devices*** from the ***Additional Hardware*** menu, or by selecting the Personal Safety toolbar button.

Toolbar Shortcut

Personal Safety Devices Overview

The Visonic SpiderAlert hardware can be used in a variety of applications. Some of these can include personal protection like in correctional facilities and schools or property protection like in museums. OnGuard classifies this hardware as Personal Safety Devices.

The Visonic SpiderAlert hardware consists of a main panel (SLC-5) that supports up to 255 bus devices. The bus devices are either receivers or input/output units. The different bus devices may also support inputs and outputs. The number of inputs and outputs vary between the device types.

SLC-5 (SpiderAlert Local Controller)

The SLC-5 is the Visonic SpiderAlert controller. The SLC-5 is the device that communicates with the PC. It can have up to 255 downstream bus devices (Receivers and Input/Output units). The SLC-5 can also have one input as well as two outputs.

When an SLC-5 is added, a pseudo alarm panel is added for this panel on the Alarm Panels form in the Alarm Panels folder. Currently the OnGuard architecture doesn't support inputs and outputs directly connected to the main panel, so part of this panel is treated as an alarm panel. The input and outputs can then be created and assigned to this alarm panel.

The SLC-5s are configured on the Personal Safety Panels form in the Personal Safety Devices folder. Configuring SLC-5s is very similar to configuring access control panels. One difference that you will see is the **Site Number** on the Personal Safety Panels form. This is basically the same thing as panel address. Each SLC-5 can be programmed with a site number. The control for the site number on this screen displays the IDs as two digit hexadecimal numbers and they are in the range 01 - FF (01 - 255 decimal).

The SLC-5 has two dip switches, SW1 and SW2. The correct settings for the dip switches depends on the action the SLC-5 is performing. The various dip switch settings are:

- Programming the SLC-5 (SW1 OFF, SW2 OFF)
- Single-Site Direct Connection to Computer (SW1 & SW2 ON)
- Multi-Site Connection via Short-Range Fast Modems (SW1 OFF, SW2 ON)
- Multi-Site Connection via Telephone-Line Modems (SW1 ON, SW2 OFF)

When configuring a Spiderbus Controller (SLC-5), the SW1 and SW2 DIP switches must be set to **OFF**. After programming of the Spiderbus Controller (SLC-5) is complete, SW1 and SW2 must be set back to **ON**.

Bus Devices

The Visonic SpiderAlert bus devices are treated as Alarm Panels. They are configured using the Alarm Panels form similar to the way Alarm Panels are configured for Access Control Panels. For more information, refer to Alarm Panels Form Procedures on page 688.

One difference is that the **Alarm Panel ID** is displayed as a two digit hexadecimal number in the range 00 - FF (0 - 255 decimal). This is because when these devices are shipped from the factory, this is how their IDs are indicated. Also, this is format that Visonic uses to refer to these IDs.

The table below lists the bus devices that are currently supported.

Bus Device Model	Description	# Inputs	#Outputs
SR-500	Single channel receiver.	3	2
SR-520	Dual technology receiver.	0	1

Bus Device Model	Description	# Inputs	#Outputs
SR-521	Dual technology receiver (Base station for SR-522 receiver).	0	1
SR-522	IR technology only receiver.	0	1
SRP-50	Spider bus signal repeater.	3	2
SRP-51	Spider bus signal repeater.	1	1
SI-540	8 output I/O unit.	0	8
SI-544	4 input and 4 output I/O unit.	4 (virtual)	4
SI-561	6 input and 1 output I/O unit.	6	1

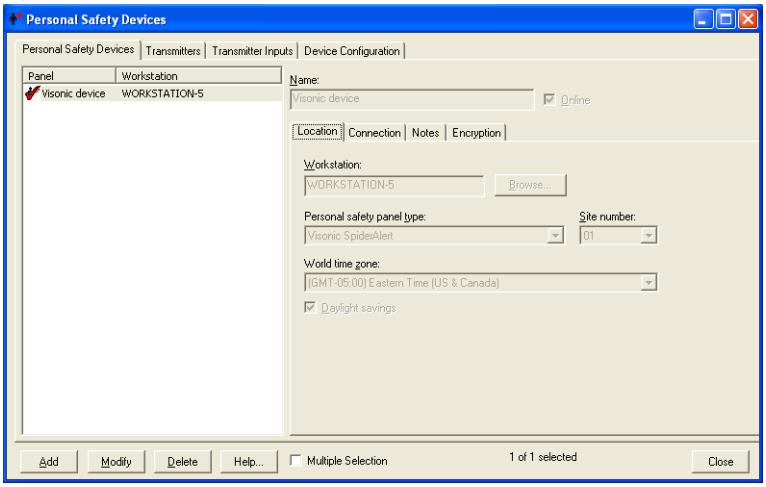
Personal Safety Devices Form

This form is used to:

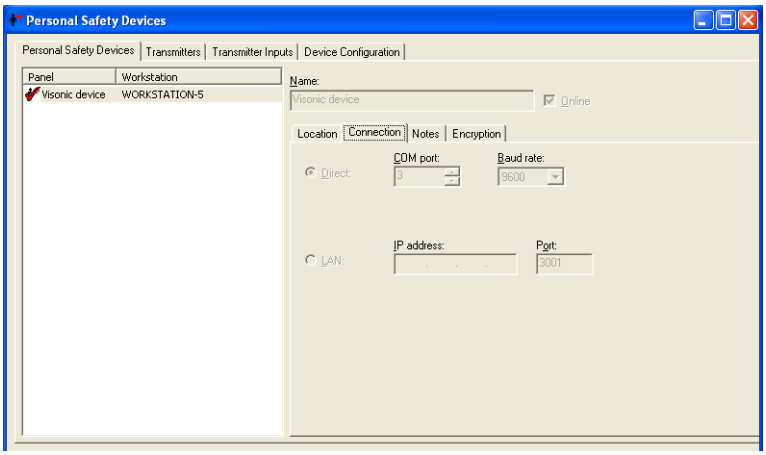
- Configure personal safety panels, including SLC-5s (Visonic SpiderAlert Local Controllers) for use in OnGuard
- Modify or delete a personal safety panel entry in OnGuard

It is important to note that dip switches 1 and 2 on the Spiderbus Controller (SLC-5) must be set to ON for direct serial connection to the SLC-5 panel.

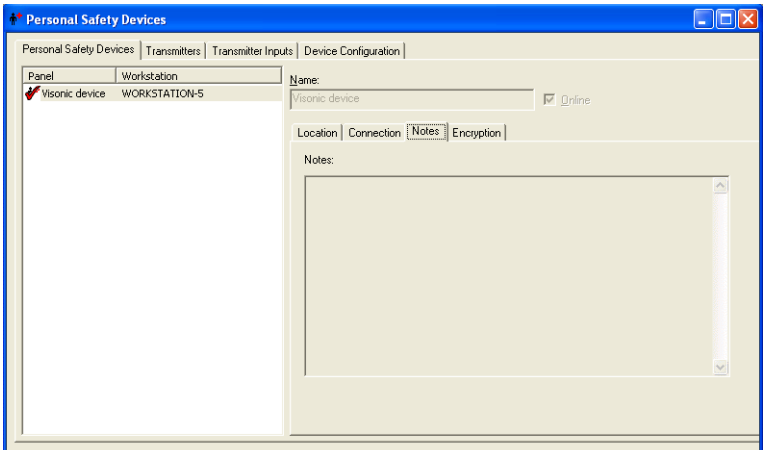
Personal Safety Devices Form (Location Sub-tab)



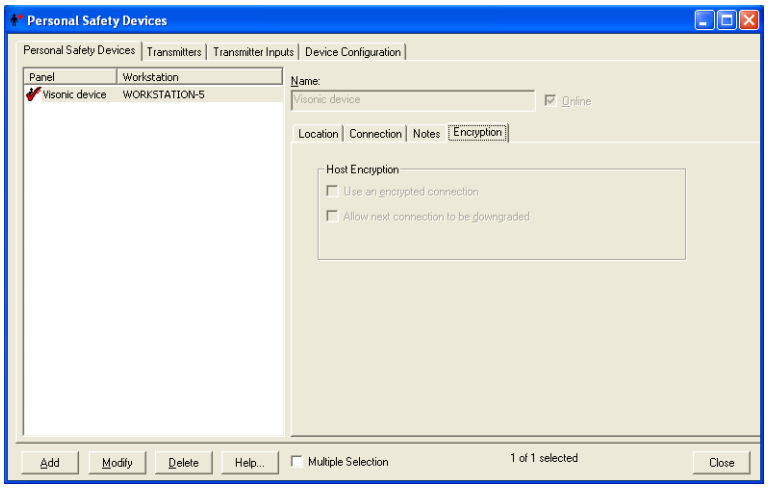
Personal Safety Devices Form (Connection Sub-tab)



Personal Safety Devices Form (Notes Sub-tab)



Personal Safety Devices Form (Encryption Sub-tab)



Note: Configuration on this tab will be disabled unless the panel is configured for a LAN connection type on the Connection sub-tab.

Personal safety devices listing window

Lists currently defined devices and the name of the workstation connected to each. A icon precedes each entry.

Name

Identifies the name of the personal safety device. This is a “friendly” name assigned to each personal safety panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the personal safety panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the device. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Add

Click on this button to add a personal safety panel.

Modify

Click on this button to change a personal safety panel.

Delete

Click on this button to delete a personal safety panel.

Help

Displays online help for this form.

Multiple Selection

If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected panels.

Mode

In view mode, indicates the record number of the selected panel, and the current total number of panels; for example, “2 of 5 selected”. In modify mode, indicates the current operation (Add Mode, Modify Mode, etc.).

Close

Closes the Personal Safety Devices folder.

Location Sub-tab

Workstation

Select the workstation or server to which the personal safety panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for computer form (see illustration on previous page) from which you can click on the name of a workstation to highlight the entry. Click on the [OK] button to then enter the workstation name in the **Workstation** field.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Personal safety panel type

Contains a list of personal safety panel types that are valid for the installed software license

Site number

Each personal safety panel can be programmed with a site number, which is similar to the panel's address. The control for the site number on the screen displays the site number as a two digit hexadecimal number. The site number can range from 01-FF (01-255 decimal).

Connection Sub-tab

Direct

Select this radio button if communication with the personal safety panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port** and **Baud rate**.

COM port

If you selected the **Direct** radio button, choose the number of the port (on the serial expansion unit or the back of the workstation or server) that will be used for communication with the panel. Choose a value in the range of 1 through 256.

Baud rate

This is the speed (in bits per second) at which information is transferred between the workstation and the personal safety panel. Currently, 9600 bps is the only baud rate supported for Visonic personal safety panels.

LAN

Select this radio button if the workstation will communicate with the personal safety panel over a Local Area Network. You must also specify the workstation's **IP address**.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the personal safety panel, as provided by your LAN Network Administrator.

An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number.

Notes Sub-tab

Notes

Enter information about the panel. This field is limited to less than 2000 characters.

Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

Encryption Sub-tab

Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key and then by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible. This check box displays only if the controller exists in an automatic key management system/segment.

Personal Safety Devices Form Procedures

Use the following procedures on this form.

Add a Personal Safety Panel

1. On the Personal Safety Devices form, click [Add].
2. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this personal safety panel will be assigned to.
   b. Click [OK].
3. In the **Name** field, type a unique, descriptive name for this panel.
4. If you want to place this panel online immediately, select the **Online** check box. Typically, you wouldn’t check this box when configuring the system or defining panels, but instead would wait until you’re ready to put the panel into service.
5. On the Location sub-tab:
   a. Enter the name of the workstation the personal safety panel will be connected to in the **Workstation** field. It’s best to select the workstation using [Browse]. In the Browse for Computer window, select the name of the workstation, then click [OK].
   b. On the Location sub-tab, Select the world time zone from the **World time zone** drop-down list.
   c. Select whether **Daylight savings** is used or not.

Note: You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

6. In the **Personal safety panel type** drop-down list, select the type of personal safety panel.
7. In the **Site Number** drop-down list, select the site number.

8. On the Connection sub-tab, select the method that will be used to communicate with the personal safety panel.
    a. Select the **Direct** radio button if communication with the personal safety panel will be via a direct serial connection to the specified **Workstation**. You must also specify the workstation's **COM port** and the **Baud rate**. Currently 9600 bps is the only baud rate supported for Visonic personal safety panels.
    b. Select the **LAN** radio button if communication with the personal safety panel will be over a Local Area Network. You must also specify the workstation's **IP address**.
9. Click [OK].

Modify a Personal Safety Panel

1. In the Personal safety devices listing window of the Personal Safety Devices form, select the entry you wish to change. To make changes to multiple entries at the same time, select the **Multiple Selection** check box and continue to select entries.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values. If the **Multiple Selection** check box is selected, the values for the **Site Number** and **Baud rate** for all selected entries will be changed to the new values.

Delete a Personal Safety Panel

1. In the Personal safety devices listing window of the Personal Safety Devices form, select the entry you wish to delete.
2. Click [Delete].
3. Click [OK].

Enable a Personal Safety Panel for Encryption

The encryption modify/export permission is required to complete this procedure. Also, encryption must be enabled and the proper encryption key configured in the communication device before enabling the panel for encryption.

1. From the ***Additional Hardware*** menu, select ***Personal Safety Devices***.
2. On the Personal Safety Devices form, click the Encryption sub-tab.
3. In the listing window, select the Personal Safety Devices entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Enter Notes for a Panel

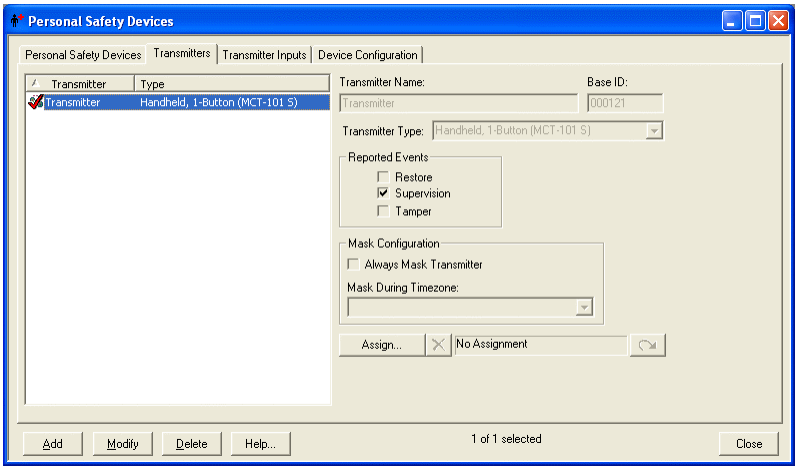
1. In the listing window, select the entry you want to edit.
2. Click [Modify].

3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Transmitters Form

The Transmitters form is used to:

- Configure transmitters that communicate with Visonic SpiderAlert receivers to be recognized by OnGuard software
- Modify or delete entries for transmitters
- Configure transmitters to be masked all the time
- Configure a transmitter to be assigned to be masked during a particular timezone
- Assign a transmitter to an asset or a cardholder



Transmitters are devices that generate an RF or IR (or both) signal that Visonic SpiderAlert receivers can receive. There are three types of these devices: fixed, portable (hand-held), and man-down. Transmitters are not assigned to any particular SLC-5; they are independent. Therefore, any receiver connected to any SLC-5 can pick up the transmitter signal.

Transmitters can be configured to be masked for a selected timezone or always masked. Transmitters can also be assigned to assets or cardholders.The various types of transmitters that OnGuard currently supports are listed below.

Model	Description
MCT-101 S	Hand held transmitter (One button).
MCT-102 S	Hand held transmitter (Two buttons).
MCT-104 S	Hand held transmitter (Four buttons).
MCT-201 S, MCT-201 WP S, MCT-201 AT S	Pendant transmitter.
MCT-211 S	Waterproof wrist transmitter.

Model	Description
MCT/IR-201 S	Dual RF & IR transmitter.
MCT-100 S	Supervised, two-input wireless transmitter.
MCT-302 S	Supervised magnetic contact transmitter.
MCT-101 MD S	Man-down transmitter.
MCT-432	Smoke Detector
MCT-501 S	Acoustic Sensor
MCT/IR-252WPS	Resettable Dual RF & IR
MDT-122 S	RF / IR man-down transmitter.
MCPIR-2000 S	Fully supervised wireless PIR detector.
MCPIR-3000 S	Full supervised wireless PIR detector.
SPD-1000	Magnetic Displacement Detector.
SPD-2000	Wireless spatial position detector.
SPD-3000	PIR Painting Removal Detector.

Transmitter Form Fields

Transmitter listing window

Lists currently defined devices and the name of the workstation connected to each. A icon precedes each entry.

Transmitter Name

Enter the name of the transmitter. This is a “friendly” name assigned to each transmitter to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Base ID

This is the base transmitter ID that is generated in the RF or IR signal that is transmitted when an event on the transmitter takes place.

- Must be specified because many transmitters can generate more than one of these signals
- Usually indicated somewhere on the transmitter, such as inside the unit
- This is a hexadecimal value that can only be made up of the following numbers or letters: 0 - 9 and A -F

Transmitter Type

This is the transmitter model.

Reported Events

Section that contains the **Restore**, **Supervision**, and **Tamper** check boxes.

- Indicates whether these events are generated for this transmitter or not.
- Can only be changed if the transmitter type that is selected has a dip switch to turn them on or off
- These settings should match the current setting of the dip switch

- Some transmitters do not have a dip switch for some of these, but they support reporting events for these so these will be displayed as checked but will not allow them to be changed.

Restore

These settings should match the current dip switch settings on the hardware.

- If checked (and the dip switches are set correctly), the transmitter will generate restore events.
- If checked and you are unable to de-select it, the transmitter supports reporting restore events, but has no dip switches for them.
- If not checked (and the dip switches are set correctly), the transmitter will not generate restore events.
- If not enabled, the transmitter does not support generating restore events.

Supervision

These settings should match the current dip switch settings on the hardware.

- If checked (and the dip switches are set correctly), the transmitter will generate supervision events.
- If checked and you are unable to de-select it, the transmitter supports reporting supervision events, but has no dip switches for them.
- If not checked (and the dip switches are set correctly), the transmitter will not generate supervision events.
- If not enabled, the transmitter does not support generating supervision events.

Tamper

These settings should match the current dip switch settings on the hardware.

- If checked (and the dip switches are set correctly), the transmitter will generate tamper events.
- If checked and you are unable to de-select it, the transmitter supports reporting tamper events, but has no dip switches for them.
- If not checked (and the dip switches are set correctly), the transmitter will not generate tamper events.
- If not enabled, the transmitter does not support generating tamper events.

Mask Configuration

Section that contains the **Always Mask Transmitter** check box and the **Mask During Timezone** drop-down list

Always Mask Transmitter

- If checked, the Communication Server will not process any message for this particular transmitter
- If not checked, the Communication Server will process any message for this particular transmitter
- When logged into System Administration in a segmented system, if the timezone for a particular segment other than the one you are logged into is currently assigned to a transmitter, this field will not be allowed to be modified
- The **Always Mask Transmitter** overrides the **Mask During Timezone** option

Mask During Timezone

- The **Mask During Timezone** option is overwritten by the **Always Mask Transmitter** option
- To mask a timezone, the **Always Mask Transmitter** check box CANNOT be selected

Assign

Click on this button to assign a transmitter to an asset or cardholder

Click on this button to delete an assignment of a transmitter to an asset or cardholder

After an assigning a transmitter to an asset or cardholder, click on this button to go to the correct screen, which displays more information about the cardholder or asset.

Add

Click on this button to add a transmitter.

Modify

Click on this button to change a transmitter.

Delete

Click on this button to delete a transmitter.

Help

Displays online help for this form.

Close

Closes the Personal Safety Devices folder

Transmitters Form Procedures

Use the following procedures on this form.

Add a Transmitter

1. On the Transmitters form, click [Add].
2. In the **Transmitter Name** field, enter a unique, descriptive name that is no longer than 32 letters.
3. In the **Base ID** field, enter the base transmitter ID that is generated when the FR or IR signal is transmitted when an event on the transmitter takes place.
4. In the **Transmitter Type** field, select a type from the drop-down list.
5. The check boxes that are applicable to the **Transmitter Type** selected will be enabled in the Reported Events section. This section indicates whether these events are generated for this transmitter or not.

   The **Restore**, **Supervision**, and **Tamper** check boxes can only be changed if the transmitter type that is selected has a dip switch to turn them on or off. The settings for these check boxes should match the current setting of the dip switch.

Some transmitters do not have a dip switch for some of the **Restore**, **Supervision**, and **Tamper** options, but they support reporting events for them. In this case, the options are displayed as checked but the application will not allow them to be changed.

6. Check the **Always Mask Transmitter** check box if you do not want the Communication Server to process any message from this particular transmitter. Otherwise, leave the **Always Mask Transmitter** check box unchecked.
7. In the **Mask During Timezone** field, select a timezone from the drop-down list if you wish to mask the transmitter during a particular timezone. For the transmitter to be masked during a timezone, the **Always Mask Transmitter** check box CANNOT be checked.

   (Note that a timezone must already have been created for it to appear in the **Mask During Timezone** drop-down list. Timezones are created on the Timezones form in the Holidays / Timezones folder.)
8. If you want to assign the timezone to an asset or cardholder, click [Assign]. See the procedures "Assign a Transmitter to an Asset" and "Assign a Transmitter to a Cardholder" for details.
9. Click [OK].

Modify a Transmitter

1. In the Transmitters listing window of the Transmitters form, select the entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Transmitter

1. In the Transmitters listing window of the Transmitters form, select the entry you wish to delete.
2. Click [Delete].
3. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Assign a Transmitter to a Cardholder

1. In the Transmitters listing window of the Transmitters form, select the entry you wish to assign a cardholder to.
2. Click [Assign].
3. The Assign Asset or Cardholder window opens. Click the **Assign [ ] Cardholder to Transmitter** radio button.
4. Click [OK], and the Cardholders folder will open.
5. On the Cardholder form in the Cardholders folder, click [Search].
6. On the Cardholders form, locate the cardholder record you want to assign the transmitter to.
7. Click on the Personal Safety Devices tab at the bottom of the window.
8. Click [Assign]. This time, the radio button will be labeled **Assign** *<name you selected>* **Cardholder to Transmitter**.
9. Select the **Assign** *<name you selected>* **Cardholder to Transmitter** radio button.
10. Click [OK]. The name of the cardholder the transmitter is assigned to will now appear in the field to the right of the button.

11. If you want to view the cardholder record that is associated with transmitter, click the button.

Assign a Transmitter to an Asset

1. In the Transmitters listing window of the Transmitters form, select the entry you wish to assign an asset to.
2. Click [Assign].
3. The Assign Asset or Cardholder window opens. Click the **Assign [-] Asset to Transmitter** radio button.
4. Click [OK], and the Assets folder will open.
5. On the Assets form in the Assets folder, click [Search].
6. On the Assets form, locate the asset record you want to assign the transmitter to.
7. Click on the Personal Safety Devices tab at the bottom of the window.
8. Click [Assign]. This time, the radio button will be labeled **Assign** *<name you selected>* **Cardholder to Transmitter**.
9. Select the **Assign** *<name you selected>* **to Transmitter** radio button.
10. Click [OK]. The name of the asset the transmitter is assigned to will now appear in the field to the right of the button.
11. If you want to view the asset record that is associated with transmitter, click the button.

Delete a Transmitter's Assignment

1. Transmitters can be assigned to either assets or cardholders. In the Transmitters listing window of the Transmitters form, select the entry that has the transmitter assignment you wish to delete.
2. Click the button, and the assignment will be deleted.

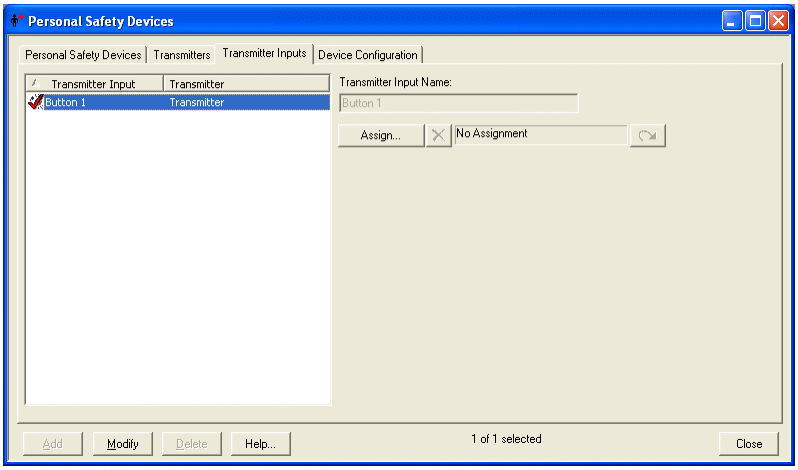
Transmitter Inputs Form

Transmitters can also have inputs. When a transmitter is added, its inputs are automatically added. Some of the transmitters have buttons, so these are named using "Button X" as opposed to "Input X" for the others.

On the Transmitter Inputs form, the names that are generated for these transmitter inputs can be modified. Transmitter inputs are not allowed to be deleted or added; only the name can be modified. Using the same form, transmitter inputs can also be assigned to assets.

The Transmitter Inputs form is used to:

- Modify the name of a transmitter input
- Assign transmitter inputs to assets



Transmitter input listing window

Lists currently defined inputs and the transmitter it is associated with. A icon precedes each entry.

Transmitter Input Name

Indicates the name of the transmitter input. The **Transmitter Input Name** is automatically created when the transmitter is added, but can be changed on this form. Each name can contain no more than 32 characters.

Assign

Click on this button to assign a transmitter input to an asset

Click on this button to delete an assignment of a transmitter input to an asset

After an assigning a transmitter input to an asset, click on this button to go to the correct screen, which displays more information about the asset.

Add

This button is disabled. Transmitter inputs cannot be added by the user; they are automatically created when a transmitter is defined.

Modify

Click on this button to modify the Transmitter Input Name or its assignment.

Delete

This button is disabled. Transmitter inputs cannot be deleted by the user.

Help

Displays online help for this form.

Close

Closes the Personal Safety Devices folder

Transmitter Inputs Form Procedures

Use the following procedures on this form.

Add a Transmitter Input

Transmitter inputs are automatically created when a transmitter is added on the Personal Safety Devices form. The user cannot directly create new transmitter inputs.

Modify a Transmitter Input

1. In the Transmitter input listing window of the Transmitter Inputs form, select the entry you wish to change.
2. Click [Modify].
3. Make the changes you want to the **Transmitter Input Name** field.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Transmitter Input

Transmitter inputs are automatically created when a transmitter is added on the Personal Safety Devices form. The user cannot delete transmitter inputs.

Assign a Transmitter Input to an Asset

1. In the Transmitter inputs listing window of the Transmitter Inputs form, select the entry you wish to assign an asset to.
2. Click [Assign].
3. The Assign Asset or Cardholder window opens. Click the **Assign [ ] Asset to Input** radio button.
4. Click [OK], and the Assets folder will open.
5. On the Assets form in the Assets folder, click [Search].
6. On the Assets form, locate the asset record you want to assign the transmitter to.
7. Click the Personal Safety Devices tab at the bottom of the window.
8. Click [Assign]. This time, the radio button will be labeled **Assign** *<name you selected>* **to Input**.
9. Select the **Assign** *<name you selected>* **to Input** radio button.
10. Click [OK]. The name of the asset the transmitter input is assigned to will now appear in the field to the right of the button.
11. If you want to view the asset record that is associated with transmitter input, click the button.

Device Configuration Form

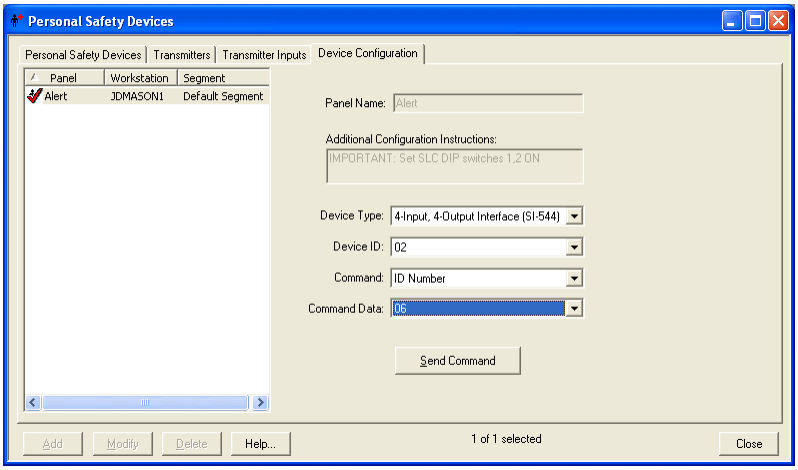
The Visonic SpiderAlert devices are shipped from the factory with default settings. The Device Configuration form has been designed for the configuration of these devices. Both the SI-561 (6-Input, 1 Output Unit) and the SRP-50 (SpiderBus Repeater) cannot be programmed and no device on

the bus after an SRP-50 can be programmed. The new SRP-51 is programmable and will allow devices after it on the bus to be programmed.

In order for any commands to be sent to the hardware, the panel needs to be configured on the Device Configuration form in the Personal Safety Devices folder. This is required so that the commands can be sent to the proper machine and panel for programming. The Communication Server must be running when programming; if it is not running the commands will fail.

When programming the main SLC-5 controller, dip switches 1 and 2 (there are only two) need to be set to OFF. To do this, the unit needs to be powered off, the dip switches set, and then the unit must be powered back up. After programming of the Spiderbus Controller (SLC-5) is complete, dip switches 1 and 2 must be set back to ON. Programming the other bus devices requires that these dip switches to be set to ON. Currently both of these switches will need to be set to ON for normal operation with the system.

When changing the SLC-5 Site ID, if the command succeeds, you will need to go back to the Visonic Configuration screen to change the site ID to match the site ID that you just changed the SLC-5 to. When changing the device ID of a bus device you will also need to make sure that you have a bus device defined for this new ID.



Device configuration listing window

Lists currently defined panels and the name of the workstation connected to each. A icon precedes each entry.

Panel Name

Identifies the name of the panel. The **Panel Name** is specified on the Personal Safety Devices form, and cannot be modified on the Device Configuration form.

Additional Configuration Instructions

After the device type is selected, instructions pertaining to the selected device are displayed here.

Device Type

Indicates the type of Visonic device. Choices include:

- SpiderBus Controller (SLC-5)
- 8-Output Interface Unit (SI-540)
- 4-Input, 4-Output Interface (SI-544)
- Wireless Receiver (SR-500)

- Dual Technology Receiver (SR-520)
- Dual Technology Receiver (SR-521)
- Dual Technology Receiver (SR-522)
- SpiderBus Repeater (SRP-51)

Device ID

- Must be specified for bus device configurations
- Represented as a two-digit hexadecimal number

Command

A function or action that will be attempt to performed at the panel when the [Send Command] button is clicked. The **Command Data** specifies the parameters for the **Command**.

Command Data

The parameters that the selected **Command** will be executed according to when both are sent to the panel by clicking the [Send Command] button.

Send Command

The Communication Server needs to be running before clicking the [Send Command] button. When this button is clicked, the selected **Command** and **Command Data** are sent to the panel.

Add

This button is disabled.

Modify

This button is disabled.

Delete

This button is disabled.

Help

Displays online help for this form.

Close

Closes the Personal Safety Devices folder

Device Configuration Form Procedures

Use the following procedures on this form.

Configure a Personal Safety Device

1. Before a personal safety device can be configured, the panel it will be associated with must be added on the Personal Safety Devices form. For more information, refer to Add a Personal Safety Panel on page 1079.
2. Make sure that the Communication Server is running. The Communication Server must be running when programming. If it is not, running the commands will fail.
3. Set the dip switches on the hardware.

a. For the SLC-5 controller, dip switches 1 and 2 (there are only two) must be set to OFF. To do this:
   - Power off the SLC-5 controller
   - Set the dip switches.
   - Power the SLC-5 back up.

b. For other bus devices, these dip switches must be set to ON

c. Both dip switches need to be set to ON for normal operation with the system.

4. In the Personal Safety Devices folder, click the Device Configuration tab.
5. In the Device configuration listing window, select the panel you wish to program a device for.
6. In the **Device Type** field, select the type of device you will be programming. Instructions pertaining to the selected device will then automatically be displayed in the **Additional Configuration** display box.
7. If the selected **Device Type** is part of a bus device configuration, a **Device ID** is required. The **Device ID** drop-down list will become enabled, and you must select a **Device ID** from the drop-down list.

   (If the selected **Device Type** is not part of a bus device configuration, it does not require a **Device ID**. In this case the **Device ID** drop-down list will not become enabled.)
8. The **Command** drop-down list will become enabled. Select a command from the drop-down list.
9. The **Command Data** drop-down list will become enabled. Select a command data time from the drop-down list.
10. Click [Send Command].
11. A message box will be displayed which asks if you are sure that you want to send the command to the selected device. Click [OK] to send the command, or click [Cancel] to not send the command.
12. A message box will be displayed indicating whether the command succeeded or failed.

CHAPTER 55

Receivers Folder

The Receivers folder contains forms with which you can:

- Add, modify, and delete receivers
- Add, modify, and delete receiver accounts (panels)
- Add, modify, and delete receiver account groups
- Add, modify, and delete zones
- Add, modify, and delete areas
- Define mappings from event codes to access control system events

The Receivers folder contains the Receivers form, Receiver Accounts form, Receiver Account Groups form, Zones form, Areas form, and the Event Code Templates form.

This folder is displayed by selecting ***Receivers*** from the ***Additional Hardware*** menu, or by selecting the Receivers toolbar button.

Toolbar Shortcut

Note: Throughout the Receivers folder documentation, the term “access control system” is used to represent the OnGuard software and hardware collectively, whereas the term “access control software” refers to only the OnGuard software.

Receivers Overview

Receivers allow the access control system to receive multiple alarms from many receiver accounts (panels) in many different formats. Receivers act as a central communication point for all of the receiver accounts configured to connect to it. Most receiver accounts communicate with the receiver via phone lines, but some also allow the communication over a direct wire or over the network.

When an event occurs on a receiver account, the receiver account dials in to a specified receiver and reports the event. The receiver accepts these messages, returns the correct handshake signals based on the specific format currently in use, formats the message, and then sends it out. Receivers typically

use a printer to maintain a hard copy of events received, but they also allow the events to be reported to the access control system. With a receiver connected to the access control system, it may monitor any receiver account that outputs in a format supported by the receiver without any configuration in the access control system.

The access control software provides an interface to display the incoming events to someone monitoring the system, and provides them with instructions on how to handle the event. This includes the use of a call list with a particular order, pass codes that need to be confirmed, etc.

The access control software receives the events from the receiver and displays them in the same manner as existing events. This allows the use of automatic paging, e-mail, custom alarms, and other additional features that the access control system provides. Instructions can be added via Alarm Configuration, and a call list may be maintained through the comments section.

Receiver Accounts Overview

Receiver accounts are used to represent panels in a receiver setup. While a receiver must be configured, receiver accounts (panels) can be added optionally. Because the receiver is between the receiver account and the access control software, there needs to be some way to represent which receiver account an event originated from. To solve this problem, an account number is entered in the receiver account, and that number is reported to the access control software.

When an event occurs for an account, Alarm Monitoring is provided with a name and other information to display. For receiver accounts that are not entered in the database initially, The access control software will automatically add them with the account number as the default name. You can then go back later and change the name.

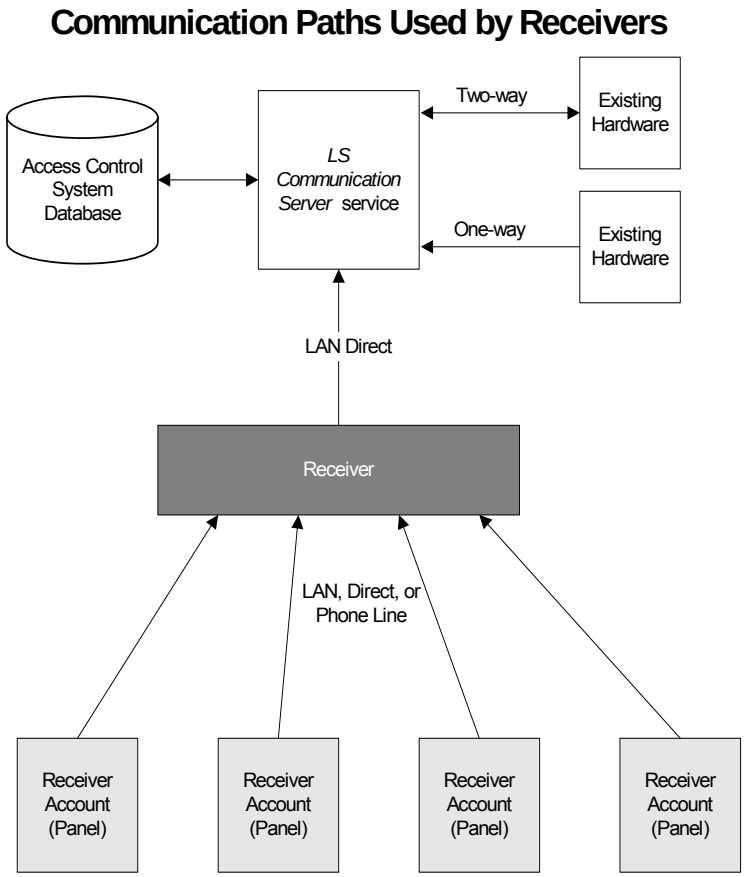
Communication Paths Used by Receivers

The connection between receiver accounts and receivers does not affect the access control system and its configuration. Receiver accounts can be connected to the receiver via a phone line, a direct wire connection, or a network connection. Data is communicated in a format that both the receiver account (panel) and the receiver understand. The receiver then formats that data into the output mode it is using and reports the information up to the access control system.

Communication between the receiver accounts and the receiver is one-way, as well as the communication between the receiver and the access control software. The access control software is only used to receive the events from the receiver and report them. All configuration of the receiver is done outside of the access control software at the receiver itself.

In a receiver/receiver account setup, the receiver is acting as the main point of communication between all receiver accounts connected to it and the access control software. For this reason, the receiver is the only piece of hardware in this setup that needs communication parameters defined in the access control software.

The following diagram illustrates the communication paths used in a receiver/receiver account setup:



Default Receiver Configuration

The following settings are the default for each receiver. These need to be set in the access control software if you are using a direct connection or in the Lantronix box if you are using a LAN connection.

Bosch D6600 (Bosch SIA and Bosch 6500):

Flow control = CTS/RTS

Baud rate = 1200

Parity = none

Byte size = 8

Stop bits = 1

Lantronix Box Communication Configuration for Receivers

To connect a receiver to the access control system over a LAN, a Lantronix box must be used. The serial settings will need to be changed based on the configuration of the receiver. The default settings

are explained in the “Default Receiver Configuration” topic in this user manual. The Lantronix box will also need the following setting configured:

Access = Remote

The following three settings are based on how IP addresses are assigned. Set all of these to disabled if a static IP Address is assigned to the Lantronix box. Otherwise, enable the appropriate flag.

- BOOTP
- RARP
- DHCP

The following three settings are based on the network the Lantronix box is connected to. They will need to be set manually or they will automatically be configured based on the three flags above.

- IP Address
- Gateway
- Subnet mask

Events Overview

The access control software receives both receiver events and account events.

- Receiver events are events that pertain to the receiver itself. These are mainly status events informing the user of any changes in the receiver’s status.
- Account events are events that are sent up from the receiver accounts to the receiver, and then reported to the access control software.

Event Code Mappings Overview

Each new receiver account connected to a receiver reports up their information in a different format. For each of these formats, there are different event codes that may represent similar events. The access control software provides a mapping between event codes received from the receivers and receiver accounts to existing access control system events.

Some receiver accounts allow event codes to be programmed into the receiver account. The meanings of these event codes are not known until they are entered in the access control software. You can enter the custom event code mappings based on how the receiver account was configured. This is done on the Event Code Templates form in the Receivers folder in the access control software.

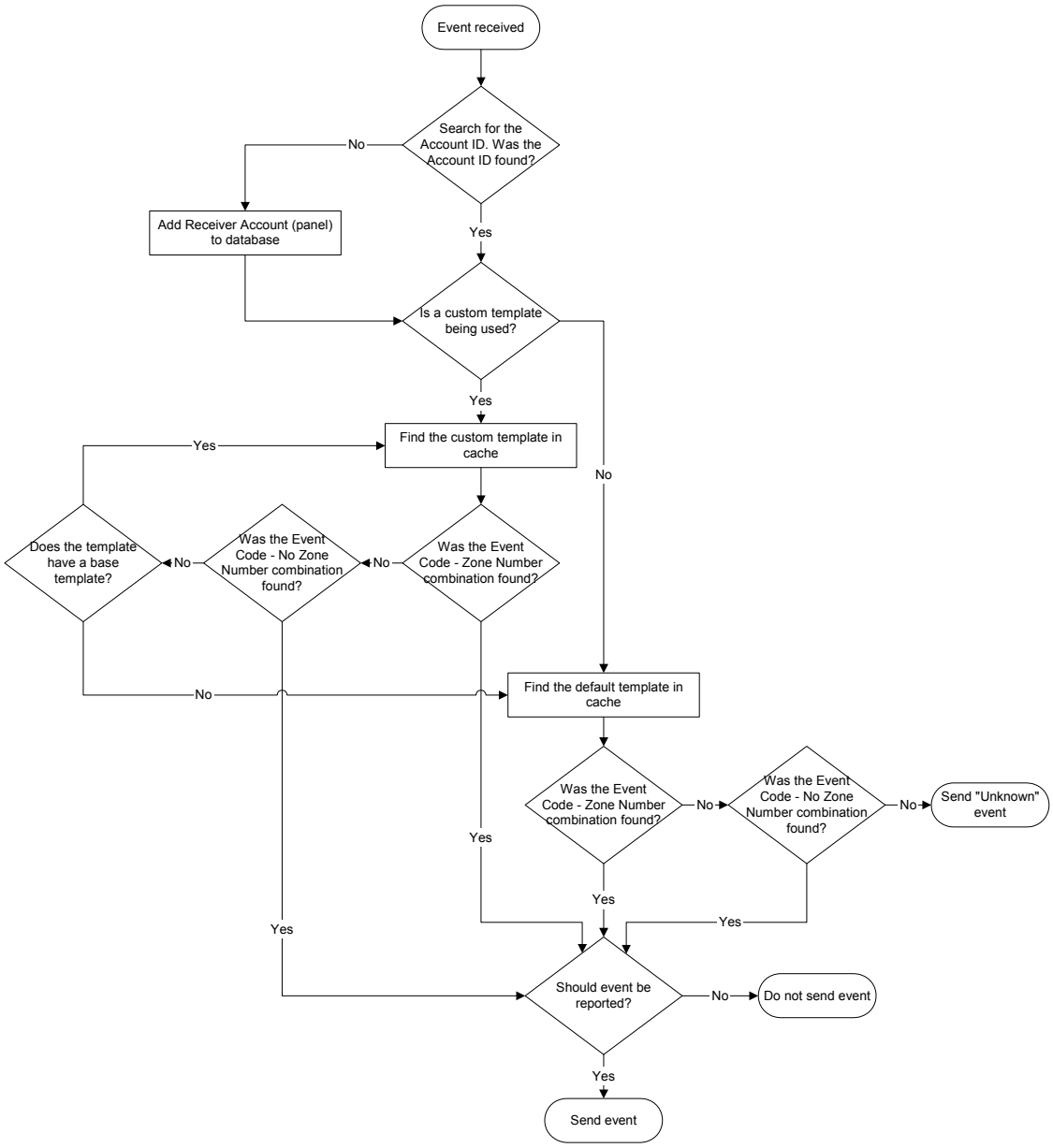
Due to the large number of events that may be generated along with the large number of receiver accounts that may be monitored with a single receiver, it is possible that a particular event code will not map to an event that corresponds to the receiver account configuration. For this reason, the way an event code maps to an event for a particular receiver account can be configured.

Event Logging and Reporting Overview

When creating and customizing the event code templates, there is also the ability to choose whether the event is reported and logged. This is useful when a receiver account is reporting up an event, perhaps quite frequently, that the user does not want to fill the database with or send to Alarm

Monitoring. If an event code is marked to not be reported/logged, that option can be overridden for a specific case using the custom event code mappings and deriving a new template off an existing template.

The following diagram shows how an event received from the receiver is processed:



Receivers Form

A receiver is a piece of hardware that the access control system can connect with to receive transactions. Each receiver must be given a name, and whether it will initially be online or not can be specified. Receivers are defined on the Receivers form by entering information on the actual Receivers form, as well as the Connection, Location, and Options sub-tabs.

Listing window

Lists currently defined receivers and the name of the workstation connected to each. A icon precedes each entry.

Name

Identifies the name of the receiver. This is a “friendly” name assigned to each receiver to make it easy to identify. Each name must be unique and can contain no more than 96 characters.

Online

If selected, the receiver will be online. Online indicates that the receiver is ready for use, and that the Communication Server will attempt to communicate with the device. If the receiver is not marked as online, the Communication Server will not attempt to communicate with the device.

Add

Click this button to add a receiver.

Modify

Click this button to change a receiver.

Delete

Click this button to delete a receiver.

Help

Displays online help for this form.

Multiple Selection

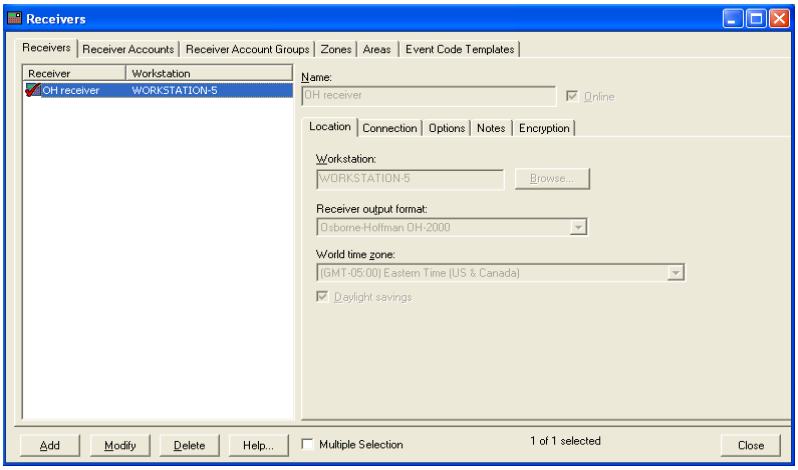
If selected, more than one Receiver entry in the listing window can be selected and modified or deleted simultaneously. Options that cannot be modified simultaneously will appear grayed out.

Close

Closes the Receivers folder

Receivers Form (Location Sub-tab)

On the Location sub-tab, you must specify the name of the **Workstation** that will be used to connect to the receiver. This is also the name of the machine running the Communication Server. This machine will be responsible for connecting with this receiver. The **Receiver output format** must also be specified.



Workstation

Select the workstation or server to which the receiver is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for computer form from which you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Receiver output format

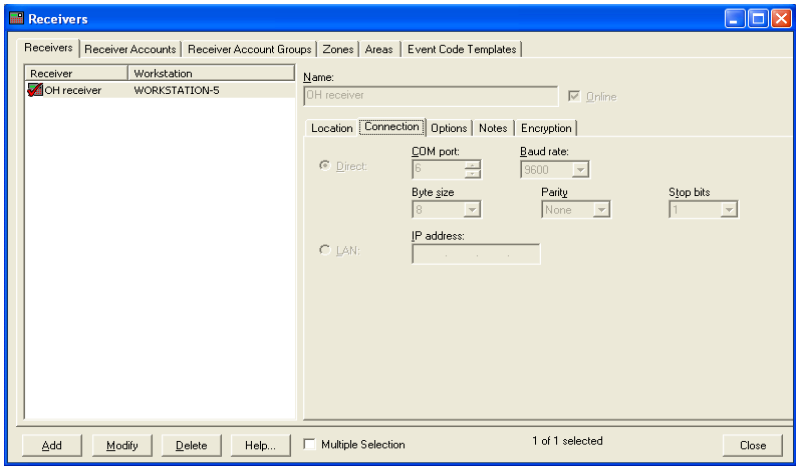
Contains a list of supported receiver output formats that are valid for the installed software license. Choices include:

- Bosch 6500
- Bosch SIA

A particular receiver output format may be supported by several different receivers. For example, the BOSCH 6500 output format is supported by the BOSCH D6500, Bosch D6600, and AES Intellinet receivers.

Receivers Form (Connection Sub-tab)

On the Connection sub-tab, you must specify how the Receiver is connected to the access control system. You can connect the Workstation via a direct serial interface. If this is chosen, the **Workstation** from the Location sub-tab must be the machine to which the direct serial connection is made. Alternatively, you can connect the Receiver to a Lantronix box and have the access control software communicate with it via a network connection. If this method is chosen the IP address of the Lantronix box must be specified.



Direct

Select this radio button if communication with the receiver will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**, **Baud rate**, **Byte size**, **Parity**, and **Stop bits**.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one receiver. Choose a value in the range of 1 through 255.

Baud rate

Enter the speed (in bits per second) at which information is transferred between the workstation and the receiver.

Byte size

Select the byte size of data transferred via the communication port. The values available for selection depend on the **Receiver output format** specified.

Parity

Select the parity of data transferred via the communication port.

Stop bits

Select the number of stop bits used in data transmission via the communication port.

LAN

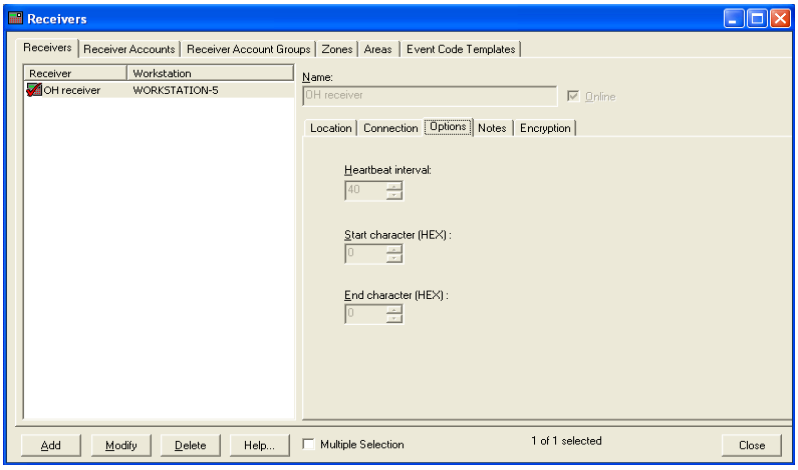
Select this radio button if the workstation will communicate with the receiver over a Local Area Network. You must also specify the workstation's **IP Address**.

IP Address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the receiver, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number.

Receivers Form (Options Sub-tab)

On the Options sub-tab, you must specify the options that the receiver must have configured correctly to communicate with the access control software. The options that must be configured depend on the **Receiver output format** specified on the Location sub-tab.



Heartbeat interval

This is the delay time between ‘heartbeat’ messages sent from the receiver to the access control system. It is used to tell the access control system that the receiver is still online. If the access control system does not receive a heartbeat message within the indicated time on that page, then the receiver is determined to be offline. This option is available for the Bosch 6500 Mode and for the Bosch SIA mode, as it is configurable on the Bosch D6600.

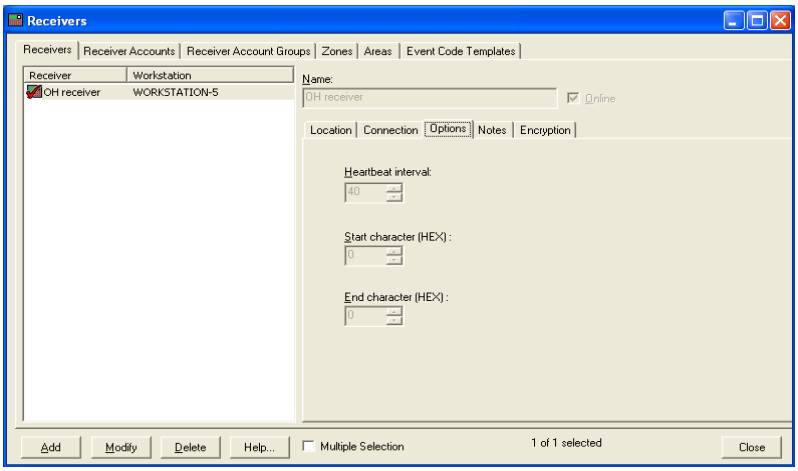
Start character (HEX)

This is available only for the Bosch 6500 Mode. For the Bosch SIA Mode, this value is hard coded as 0x0a. The Bosch D6600 allows you to configure the header character for 6500 Mode messages. This needs to be configured properly for the access control system to communicate with the receiver.

End character (HEX)

This is available only for the Bosch 6500 Mode. For the Bosch SIA Mode, this value is hard coded as 0x0d. The Bosch D6600 allows you to configure the trailer character for 6500 Mode messages. This needs to be configured properly for the access control system to communicate with the receiver.

Receivers Form (Notes Sub-tab)

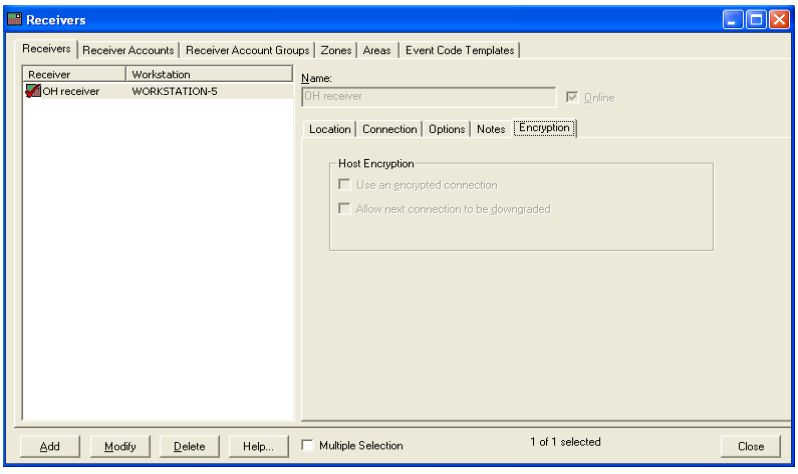


Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

Receivers Form (Encryption Sub-tab)

The Encryption sub-tab displays when the system/segment (the panel is associated with) uses automatic encryption. The same fields display when the system/segment is configured for manual encryption, except for the **Allow next connection to be downgraded** check box.The Encryption sub-tab does not display if a system/segment uses a plain connection. For more information about encryption, refer to the Encryption for Controllers User Guide.



Note: Configuration on this tab will be disabled unless the panel is configured for a LAN connection type on the Connection sub-tab.

Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key and then by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible.

This check box displays only if the controller exists in an automatic key management system/ segment.

Receivers Form Procedures

Use the following procedures on this form.

Add a Receiver

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. On the Receivers tab, click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this receiver will be assigned to.
   b. Click [OK].
4. In the **Name** field, type a name for the receiver.
5. Select whether the receiver will be online.
   a. Allow the **Online** check box to remain selected if you want the receiver to be ready for use. When a receiver is online, the Communication Server will attempt to communicate with the device.
   b. Deselect the **Online** check box if the receiver is not ready for use. If the receiver is not marked as online, the Communication Server will not attempt to communicate with the device.
6. On the Location sub-tab:
   a. Select the **Workstation** (or server) to which the receiver is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use [Browse] to view a list of available workstations.
   b. Select the world time zone from the **World time zone** drop-down list.
   c. Select whether **Daylight savings** is used or not.

Note: You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

7. In the **Receiver output format** drop-down list, select a receiver output format that is valid for the installed software license.
8. Click the Connection sub-tab.
9. Select the method that will be used to communicate with the receiver.

a. Select the **Direct** radio button if communication with the receiver will be via a direct serial connection to the specified **Workstation**. You must also specify the workstation's **COM Port**, the **Baud rate**, the **Byte size**, the **Parity**, and the **Stop bits**.

b. Select the LAN radio button if communication with the receiver will be over a Local Area Network. You must also specify the workstation's IP address.

10. Click the Options sub-tab. Different options are available depending on the **Receiver output format** that you selected on the Location sub-tab. Options not available are grayed out.

    a. If the Receiver output format is **Bosch 6500**, select the **Heartbeat interval**, the **Start character (HEX)**, and the **End character (HEX)**.

    b. If the Receiver output format is **Bosch SIA**, select the **Heartbeat interval**.

11. Click [OK].

Modify a Receiver

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. On the Receivers tab, select the **Multiple Selection** check box if you want to modify more than one Receiver entry. If not, leave it deselected.
3. Select the Receiver entry you want to modify. If the **Multiple Selection** check box is selected, you can select more than one Receiver entry.
4. Click [Modify].
5. Make any desired changes.
6. Click [OK].
7. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

Delete a Receiver

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. On the Receivers tab, select the **Multiple Selection** check box if you want to delete more than one Receiver entry. If not, leave it deselected.
3. Select the Receiver entry you want to delete. If the **Multiple Selection** check box is selected, you can select more than one Receiver entry.
4. Click [Delete].
5. Click [OK].
6. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

Enable a Receiver for Encryption

The encryption modify/export permission is required to complete this procedure. Also, encryption must be enabled and the proper encryption key configured in the communication device before enabling the panel for encryption.

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. On the Receiver form, click the Encryption sub-tab.
3. In the listing window, select the Receiver entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.

6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Enter Notes for a Receiver

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Receiver Accounts Form

On the Receiver Accounts form, you can specify receiver accounts (panels). A receiver account must have a **Name** and an **Account number** defined. The **Name** can be any user-friendly name, and is what is displayed in Alarm Monitoring. The **Account number** must match the account number as reported from the receiver. The Options sub-tab contains fields for optional information that may be associated with the receiver account.

If the access control software receives a transaction for a receiver account that has not been defined, it will automatically add a receiver account for it and fill in the **Account number** and **Name**. The **Account number** is the exact number as reported from the receiver.

Receiver Account listing window
Lists currently defined receiver accounts.

Name
Identifies the name of the receiver account. This is a “friendly” name assigned to each account to make it easy to identify. This name will be displayed in Alarm Monitoring. Each name must be unique and can contain no more than 96 characters.

Account number
The **Account number** must match the account number as reported from the receiver.

Add
Click this button to add a receiver account.

Modify
Click this button to change a receiver account.

Delete
Click this button to delete a receiver account.

Help
Displays online help for this form.

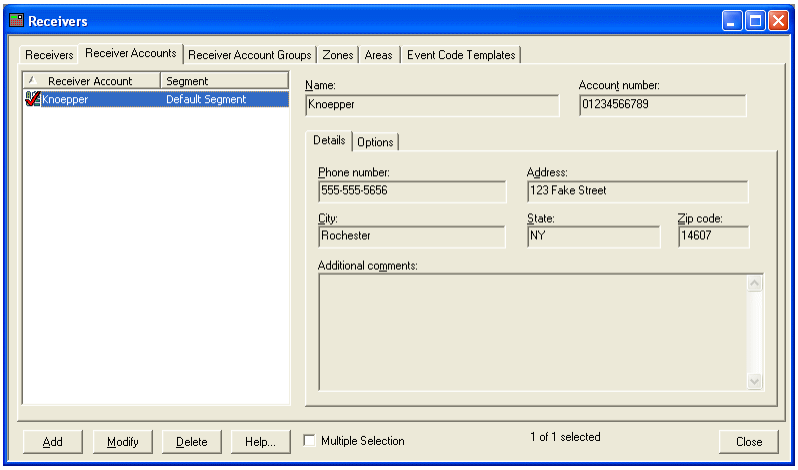
Multiple Selection

If selected, more than one Receiver Account entry in the listing window can be selected and modified or deleted simultaneously. Options that cannot be modified simultaneously will appear grayed out.

Close

Closes the Receivers folder

Receiver Accounts Form (Details Sub-tab)



Phone number

(Optional) Telephone number associated with the receiver account

Address

(Optional) Address associated with the receiver account

City

(Optional) City associated with the receiver account

State

(Optional) State associated with the receiver account

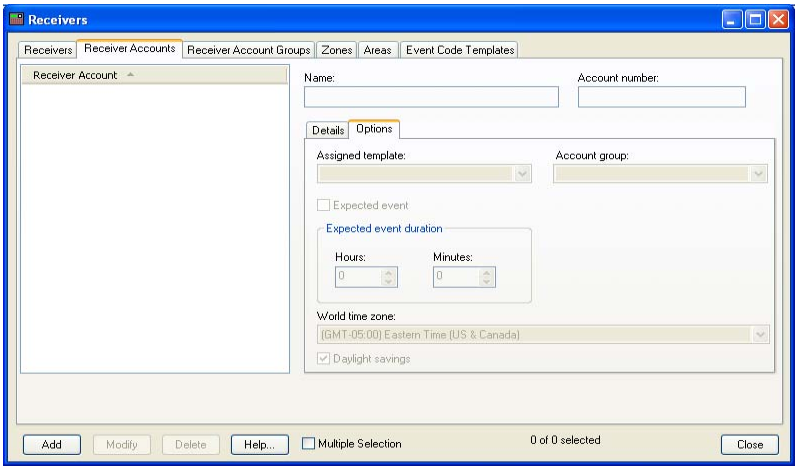
Zip code

(Optional) Zip code associated with the receiver account

Additional comments

(Optional) Type any additional information about the receiver account here. There is a limit of 32,000 characters.

Receiver Accounts Form (Options Sub-tab)



Assigned template

Used to specify custom mappings for event codes reported from the receiver for the given receiver account to access control system event definitions. If an assigned template is not selected, the access control system will use a default template.

Expected event

Select this check box to indicate that an event will take place. When selected, the **Hours** and **Minutes** fields are available for selection.

Expected event duration

Section that contains the **Hours** and **Minutes** fields. This section is only enabled when the Expected event check box is selected.

Hours

Specify the number of hours that event will go on for

Minutes

Specify the number of minutes, in addition to the specified **Hours**, that the event will go on for

Account group

Select the account group that this receiver account will be a member of, if any. Receiver Account Groups are added on the Receiver Account Groups form in the Receivers folder. If segmentation is enabled, the Receiver Account Group must be in the same segment as the Receiver in order to be available for selection in the **Account group** drop-down list.

The **Account group** specified will appear on the Account List sub-tab of the Receiver Account Groups form when that same Receiver Account Group is selected in the Receiver Account Group listing window of the Receiver Account Groups form.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Receiver Accounts Form Procedures

Use the following procedures on this form.

Add a Receiver Account

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Receiver Accounts tab.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this receiver account will be assigned to.
   b. Click [OK].
5. In the **Name** field, type a name for the receiver account.
6. In the **Account number** field, type the account number as reported from the receiver. Each receiver has a unique account number.
7. On the Details sub-tab, fill in any options associated with the receiver account. No options are required, but you can enter the **Phone number**, **Address**, **City**, **State**, **Zip code**, and any **Additional comments**.
8. On the Options sub-tab:
   a. You can select an **Assigned template**. An assigned template is used to specify custom mappings for event codes reported from the receiver for the given receiver account to access control system event definitions.

      If an assigned template is not selected, the access control system will use a default template.
   b. You can also select if an event is expected to occur. If an event is expected, enter the number of **Hours** and **Minutes** that the event will go on for.
   c. Select the **Account group** that the receiver account will belong to, if any.
   d. Select the world time zone and daylight savings options as you see fit.

Note: Receiver Account Groups are added on the Receiver Account Groups form in the Receivers folder. If segmentation is enabled, the Receiver Account Group must be in the same segment as the Receiver in order to be available for selection in the **Account group** drop-down list. For more information, refer to Add a Receiver Account Group on page 1111.

9. Click [OK].

Modify a Receiver Account

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Receiver Accounts tab.
3. Select the **Multiple Selection** check box if you want to modify more than one Receiver Account entry. If not, leave it deselected.

4. Select the Receiver Account entry you want to modify. If the **Multiple Selection** check box is selected, you can select more than one Receiver Account entry.
5. Click [Modify].
6. Make any desired changes. Changes can be made on any sub-tab.
7. Click [OK].
8. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

Delete a Receiver Account

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Receiver Accounts tab.
3. Select the **Multiple Selection** check box if you want to delete more than one Receiver Account entry. If not, leave it deselected.
4. Select the Receiver Account entry you want to delete. If the **Multiple Selection** check box is selected, you can select more than one Receiver Account entry.
5. Click [Delete].
6. Click [OK].
7. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

Receiver Account Groups Form

Receiver Account Group listing window

Lists currently defined receiver account groups. A icon precedes each entry.

Name

Identifies the name of the receiver account group. This is a “friendly” name assigned to each account to make it easy to identify. This name will be displayed in Alarm Monitoring. Each name must be unique and can contain no more than 96 characters.

Add

Click this button to add a receiver account group.

Modify

Click this button to change a receiver account group.

Delete

Click this button to delete a receiver account group.

Help

Displays online help for this form.

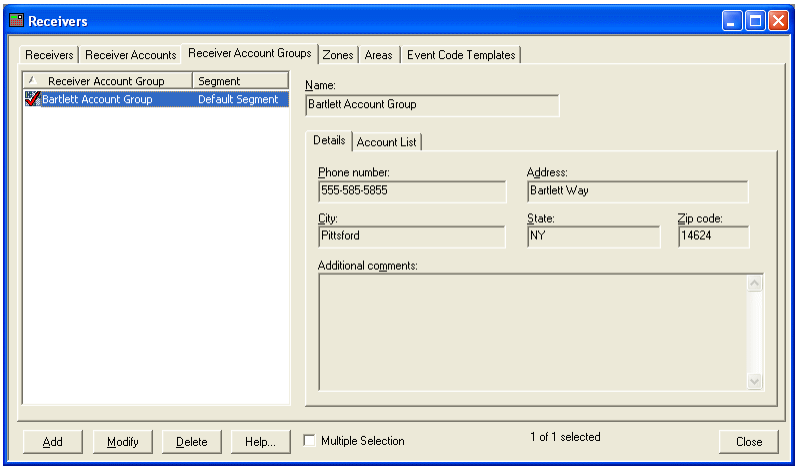
Multiple Selection

If selected, more than one Receiver Account Group entry in the listing window can be selected and modified or deleted simultaneously. Options that cannot be modified simultaneously will appear grayed out.

Close

Closes the Receivers folder

Receiver Account Groups Form (Details Sub-tab)



Phone number

(Optional) Telephone number associated with the receiver account group

Address

(Optional) Address associated with the receiver account group

City

(Optional) City associated with the receiver account group

State

(Optional) State associated with the receiver account group

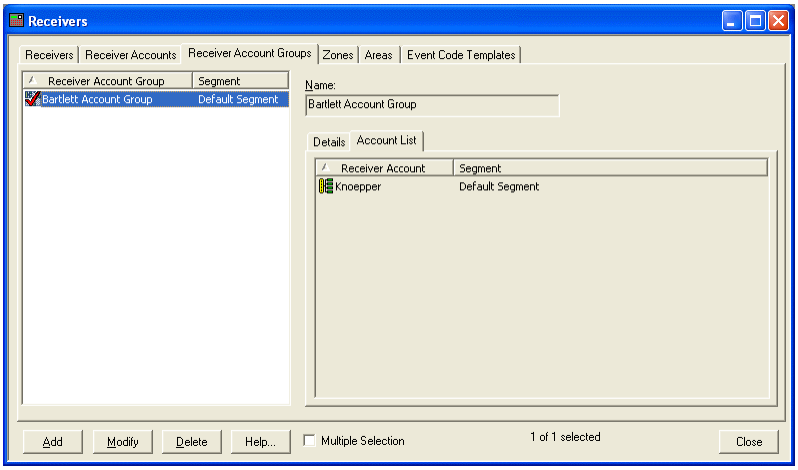
Zip code

(Optional) Zip code associated with the receiver account group

Additional comments

(Optional) Type any additional information about the receiver account group here. There is a limit of 32,000 characters.

Receiver Account Groups Form (Account List Sub-tab)



Account List listing window

For a receiver account group that is selected in the Receiver Account Group listing window, lists the names of receiver accounts and the segment each belongs to. For a Receiver Account to be listed, the Receiver Account Group that is selected in the Receiver Account Group listing window on this form must also be selected in the **Account group** drop-down list on the Receiver Accounts form.

Receiver Accounts Form Procedures

Use the following procedures on this form.

Add a Receiver Account Group

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Receiver Account Groups tab.
3. Click [Add].
4. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this receiver account group will be assigned to.
   b. Click [OK].
5. In the **Name** field, type a name for the receiver account group.
6. On the Details sub-tab, fill in any options associated with the receiver account group. No options are required, but you can enter the **Phone number**, **Address**, **City**, **State**, **Zip code**, and any **Additional comments**.
7. On the Account List sub-tab, the list of receiver accounts and the segment that the selected receiver account group belongs to. For a Receiver Account to be listed, the Receiver Account Group that is selected in the Receiver Account Group listing window on this form must also be selected in the **Account group** drop-down list on the Receiver Accounts form.
8. Click [OK].

Modify a Receiver Account Group

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Receiver Account Groups tab.
3. Select the Receiver Account Group entry you want to modify.
4. Click [Modify].
5. Make any desired changes. Changes can be made on any sub-tab.
6. Click [OK].
7. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

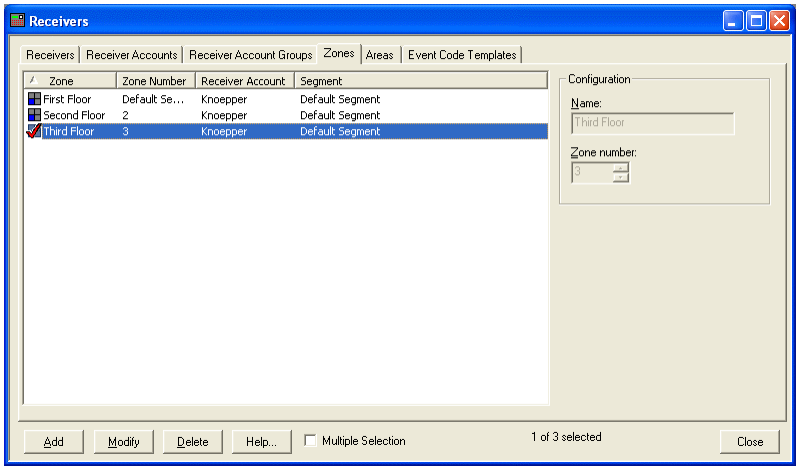
Delete a Receiver Account Group

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Receiver Account Groups tab.
3. Select the Receiver Account Group entry you want to delete.
4. Click [Delete].
5. Click [OK].
6. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

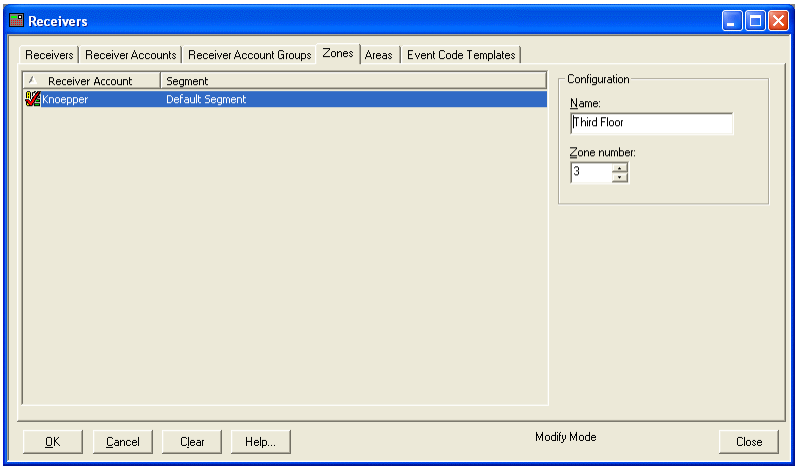
Zones Form

Various receiver accounts allow you to define zones. When an event occurs on a receiver account, the receiver account reports up its account number, the event that occurred, the zone information, and any additional information that may be supported by the receiver account. Zones can be configured in the access control software and given an appropriate name. When the access control software receives a receiver account event with this information, Alarm Monitoring will display the names associated with a particular zone. If a zone does not have a name defined for it, then the access control software will use the raw hardware ID it received.

Zones Form (View Mode)



Zones Form (Modify Mode)



Listing window (view mode)

Lists currently defined areas as well as the **Area number**, **Receiver Account**, and **Segment** (if segmentation is enabled) they are associated with. An icon precedes each entry.

Listing window (modify mode)

Lists currently defined receiver accounts that you can assign to an area or areas. An icon precedes each entry.

Configuration

Includes the **Name** field and **Area number** spin button field.

Name

The name of the **Area**. This is the name that will be displayed in Alarm Monitoring. If the access control software receives an account event with area information in it but the area doesn't have a name, the raw hardware ID will be used instead.

Area number

Each area is assigned a number.

Add (view mode)

Click this button to add an area.

Modify (view mode)

Click this button to change an area.

Delete (view mode)

Click this button to delete an area.

OK (modify mode)

Click the [OK] button once you are finished to apply the changes that were made.

Cancel (modify mode)

Cancels any action initiated and reverts to the previously saved values.

Clear (modify mode)
Clears the current form.

Help
Displays online help for this form.

Multiple Selection
If selected, more than one Area entry in the listing window can be selected and deleted simultaneously.

Close
Closes the Receivers folder

Zones Form Procedures

Use the following procedures on this form.

Add a Zone

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Add any Receiver Accounts you want to create zones for. For more information, refer to Add a Receiver Account on page 1108.
3. Click the Zones tab.
4. Click [Add].
5. All receiver accounts will be displayed in the listing window.
6. Select the Receiver Account entry you want to create a zone for.
7. In the **Name** field, type the name of the Zone. This is the name that will be displayed in Alarm Monitoring.

Note: If the access control software receives an account event with zone information in it but the zone doesn't have a name, the raw hardware ID will be used instead.

8. Select the **Zone number**. A **Zone number** is individual input point on a receiver account, and each zone must have one. More than one receiver account can be assigned to the same zone number.

Note: Unless you are using Osborne-Hoffman OH2000 hardware, OnGuard does not support zone numbers that are set to 0 and should not be configured as such. If a panel treats a zone as zero it will not be reported on correctly. If you are using Osborne-Hoffman OH2000 hardware a zone 0 event will be reported as zone 32767.

9. Click [OK].

Modify a Zone

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Zones tab.
3. Select the Zone entry you want to modify.
4. Click [Modify].

5. Make any desired changes.
6. Click [OK].
7. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

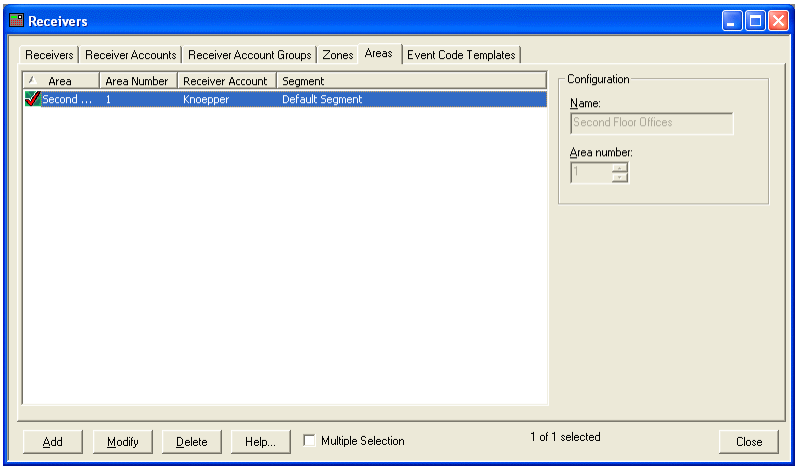
Delete a Zone

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Zones tab.
3. Select the **Multiple Selection** check box if you want to delete more than one Zone entry. If not, leave it deselected.
4. Select the Zone entry you want to delete. If the **Multiple Selection** check box is selected, you can select more than one Zone entry.
5. Click [Delete].
6. Click [OK].
7. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

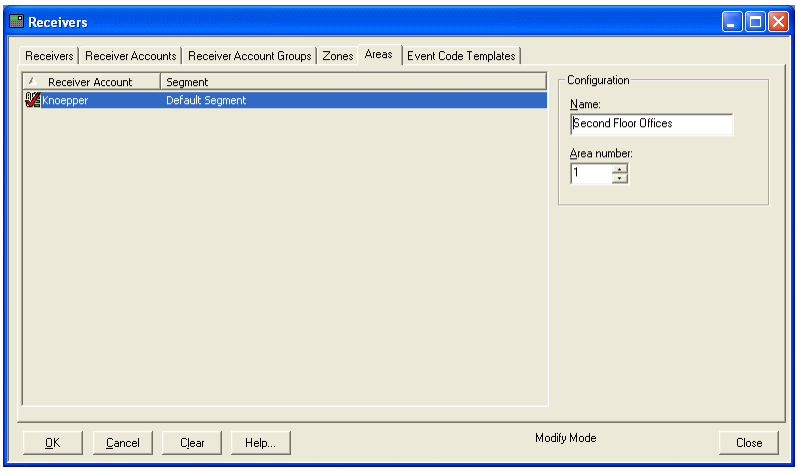
Areas Form

Various receiver accounts allow you to define areas. When an event occurs on a receiver account, the receiver account reports up its account number, the event that occurred, the area information, and any additional information that may be supported by the receiver account. Areas can be configured in the access control software and given an appropriate name. When the access control software receives a receiver account event with this information, Alarm Monitoring will display the names associated with a particular area. If an area does not have a name defined for it, then the access control software will use the raw hardware ID it received.

Areas Form (View Mode)



Areas Form (Modify Mode)



Listing window (view mode)

Lists currently defined areas as well as the **Area number**, **Receiver Account**, and **Segment** (if segmentation is enabled) they are associated with. An icon precedes each entry.

Listing window (modify mode)

Lists currently defined receiver accounts that you can assign to an area or areas. An icon precedes each entry.

Configuration

Includes the **Name** field and **Area number** spin button field.

Name

The name of the **Area**. This is the name that will be displayed in Alarm Monitoring. If the access control software receives an account event with area information in it but the area doesn't have a name, the raw hardware ID will be used instead.

Area number

Each area is assigned a number.

Add (view mode)

Click this button to add an area.

Modify (view mode)

Click this button to change an area.

Delete (view mode)

Click this button to delete an area.

OK (modify mode)

Click the [OK] button once you are finished to apply the changes that were made.

Cancel (modify mode)

Cancels any action initiated and reverts to the previously saved values.

Clear (modify mode)
Clears the current form.

Help
Displays online help for this form.

Multiple Selection
If selected, more than one Area entry in the listing window can be selected and deleted simultaneously.

Close
Closes the Receivers folder

Areas Form Procedures

Use the following procedures on this form.

Add an Area

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Add any Receiver Accounts you want to create areas for. For more information, refer to Add a Receiver Account on page 1108.
3. Click the Areas tab.
4. Click [Add].
5. All receiver accounts will be displayed in the listing window.
6. Select the Receiver Account entry you want to create an area for.
7. In the **Name** field, type the name of the Area.

Note: If the access control software receives an account event with area information in it but the area doesn't have a name, the raw hardware ID will be used instead.

8. Select the **Area number**.
9. Click [OK].

Modify an Area

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Areas tab.
3. Select the Area entry you want to modify.
4. Click [Modify].
5. Make any desired changes.
6. Click [OK].
7. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

Delete an Area

1. From the ***Additional Hardware*** menu, select ***Receivers***.

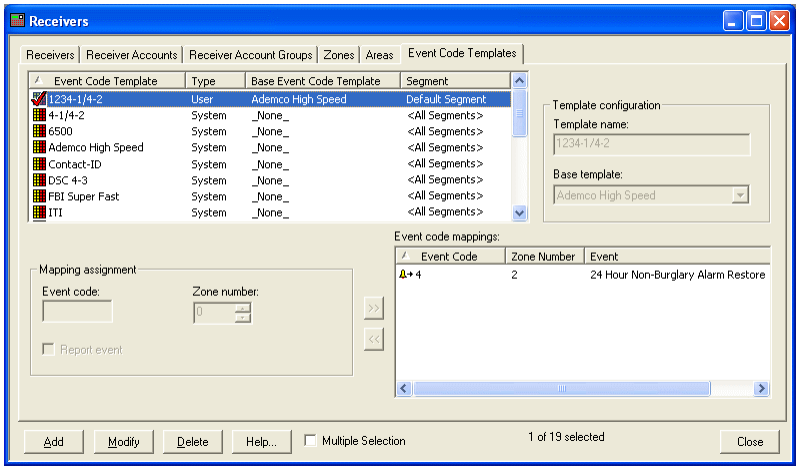
2. Click the Areas tab.
3. Select the **Multiple Selection** check box if you want to delete more than one Area entry. If not, leave it deselected.
4. Select the Area entry you want to delete. If the **Multiple Selection** check box is selected, you can select more than one Area entry.
5. Click [Delete].
6. Click [OK].
7. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

Event Code Templates Form

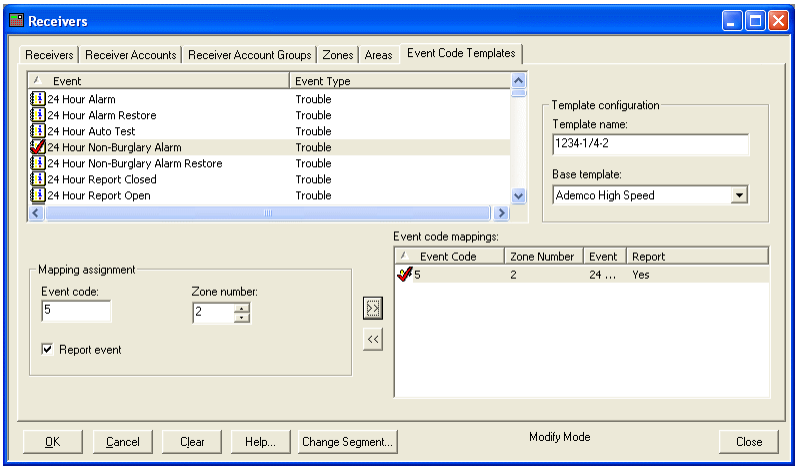
On the Event Code Templates form, you can define mappings from event codes to access control system events. A table (called an Event Code Template) of such mappings can be defined and then assigned to the given account zone(s).

- Several system default mappings come with the access control software.
- New templates can be added.
- Existing mappings (including default ones) can be customized by defining a new template, basing it off an existing one, and then defining overrides. The mapping can be done down to the zone level.

Event Code Templates Form (View Mode)



Event Code Templates Form (Modify Mode)



Listing window (view mode)

Lists currently defined event code templates as well as the **Type** and **Base event code template** they are associated with. A icon precedes each entry. Event code templates with a **Type** of "System" cannot be modified, but event code templates with a **Type** of "User" can be modified.

Listing window (modify mode)

Lists currently defined events as well as the **Event Type** they are associated with. A icon precedes each entry.

Template configuration

Includes the **Template name** field and **Base template** drop-down list.

Template name

The name of the **Event code template**, which is a table of mappings from event codes to access control system events

Base template

The original template that a new template is derived from

Mapping assignment

Includes the **Event code** field, the **Zone number** spin-button field, and the **Report event** check box.

Event code

An alphanumeric value reported from the receiver for the given receiver account to access control system event definitions. An event code can have a space at the beginning or anywhere in it, but it cannot have a trailing space. For example, "A D01" and " AS" are valid event codes, but "A " is not a valid event code because it has a space at the end.

Zone number

Each zone, or individual input point on a receiver account, is assigned a number. When the **Zone number** is zero (0), any zone will match if a search is done.

Report event

If selected, events will be reported to the access control software and logged. If not selected, events will not be reported to the access control software and will not be logged.

Event code mappings

Displays the **Event Code**, **Zone number**, and **Event** pairings, as well as whether the mapping is reported or not.

When clicked, the selected Event, the **Event code** specified and the **Zone number** selected are linked and added to the **Event code mappings** display

When clicked, the **Event code mapping** that is selected is removed

Add (view mode)

Click this button to add an event code template.

Modify (view mode)

The **Type** of the Event Code Template (displayed in the listing window) determines whether it can be modified - “System” event code templates cannot be modified, but “User” event code templates can be.

Delete (view mode)

The **Type** of the Event Code Template (displayed in the listing window) determines whether it can be deleted - “System” event code templates cannot be deleted, but “User” event code templates can be.

OK (modify mode)

Click the [OK] button, once you are finished, to apply the changes that were made.

Cancel (modify mode)

Cancels any action initiated and reverts to the previously saved values.

Clear (modify mode)

Clears the current form.

Help

Displays online help for this form.

Multiple Selection

If selected, more than one entry in the listing window with the Type “User” can be checked simultaneously. The changes made on this form will apply to all selected event code templates.

The **Multiple Selection** check box cannot be used for entries with the Type “System”, since those entries cannot be modified or deleted.

If segmentation is enabled, the event code templates must be in the same segment to be able to use the Multiple Selection feature.

Close

Closes the Receivers folder.

Event Code Templates Form Procedures

Use the following procedures on this form.

Add a Custom Event Code Template

The access control software comes with the most commonly used event code templates. There are three instances where you might want to add a custom event code template:

- Scenario 1: If your receiver account uses an event code template other than the default ones, you will have to add a new event code template that specifies the event code mappings. If you do not do this, then any events that the receiver account sends will be listed as “Unknown” in Alarm Monitoring.
- Scenario 2: The default event code templates that come with the access control software have a **Type** of “System”. System event code templates cannot be modified. To override one of the event code mappings present in a system event code template, you can add a new event code template based on that same system account.
- Scenario 3: If you do not want an event to be reported that is included in a system event code template, then you can add a new event code template in which the **Report event** check box is deselected for that event.

To add a custom event code template:

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Event Code Templates tab.
3. In the Event Code Template listing window, select the template you want to base your new template on. Make note of the event code mappings that you wish to override. (If you are adding a completely new event code template, as in Scenario 1 above, you do not have to select a template.)
4. Click [Add].
5. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window will open. Select the segment that this event code template will be assigned to.
   b. Click [OK].
6. In the **Template name** field, type a new name for the template.
7. In the **Base template** field, select the template that the new event code template will be derived from. In most cases, this will be the template that you selected in step 3.
8. In the Event listing window, select the event you want to be paired with the event code and zone number.
9. In the **Event code** field, specify the event code. Usually this is an event code that is listed in the **Base template** that you want to reassign. An event code can have a space at the beginning or in the middle, but it cannot have a space at the end.
10. Enter the **Zone number**.
11. Select the **Report event** check box if you want events to be reported to Alarm Monitoring and logged, or deselect it to not have events reported or logged.
12. Click the button, and the event code mapping will be added.

For more information, refer to Event Logging and Reporting Overview on page 1096.

- Default system event code templates have a **Type** of “System”.

- Custom event code templates have a **Type** of “User”.

Modify an Event Code Template

User-defined event code templates can be modified, but the default event code templates that come with the access control software cannot. To modify an event code template:

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Event Code Templates tab.
3. Select the **Multiple Selection** check box if you want to modify more than one Event Code Template entry. If not, leave it deselected.
4. In the Event Code Template listing window, select the template with a **Type** of “User” that you want to modify. If the **Multiple Selection** check box is selected, you can select more than one Event Code Template entry. Make note of the event code mappings that you wish to override.
5. Click [Modify].
6. Make any desired changes.
7. Click [OK].
8. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

Delete an Event Code Template

User-defined event code templates can be deleted, but the default event code templates that come with the access control software cannot. To delete an event code template:

1. From the ***Additional Hardware*** menu, select ***Receivers***.
2. Click the Event Code Templates tab.
3. Select the **Multiple Selection** check box if you want to delete more than one Event Code Template entry. If not, leave it deselected.
4. In the Event Code Template listing window, select the template with a **Type** of “User” that you want to delete. If the **Multiple Selection** check box is selected, you can select more than one Event Code Template entry.
5. Click [Delete].
6. Click [OK].
7. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

CHAPTER 56

Intrusion Detection Devices Folder

The Intrusion Detection Devices folder contains forms with which you can:

- Add, modify, and delete intrusion panels.
- Define objects (zones, onboard and offboard relays, doors, and areas) relating to each intrusion panel.
- Add, modify, and delete panel user groups.

The Intrusion Detection Devices folder contains the Intrusion Panels form, Zones form, Onboard Relays form, Offboard Relays form, Doors form, Areas form, and the Panel User Groups form.

This folder is displayed by selecting ***Intrusion Detection Devices*** from the ***Additional Hardware*** menu, or by selecting the Intrusion Detection toolbar button.

Toolbar Shortcut

Intrusion Panels Form

OnGuard is designed to interface with intrusion controllers and to request the controllers to perform supported actions (such as bypass/unbypass zone, activate/deactivate an output and arm/disarm an area).

Implementation of Detection System products and Galaxy products requires the configuration using their respective keypads as well as the configuration of OnGuard components using OnGuard software. Refer to the manufacturer manuals when configuring the panel with the keypad.

Implementation of Bosch products requires the configuration of the Bosch components using Bosch software as well as the configuration of OnGuard components using OnGuard software. Refer to the Bosch manuals when working with Bosch software.

Listing window

Lists currently defined intrusion panels and the name of the workstation connected to each. A icon precedes each entry.

Name
Identifies the name of the intrusion panel. This is a “friendly” name assigned to each intrusion panel to make it easy to identify. Each name must be unique and can be up to 32 characters long.

Online
If selected, the intrusion panel will be online. Online indicates that the intrusion panel is ready for use, and that the Communication Server will attempt to communicate with the device. If the intrusion panel is not marked as online, the Communication Server will not attempt to communicate with the device.

Add
Click this button to add an intrusion panel.

Modify
Click this button to modify an intrusion panel.

Delete
Click this button to delete an intrusion panel.

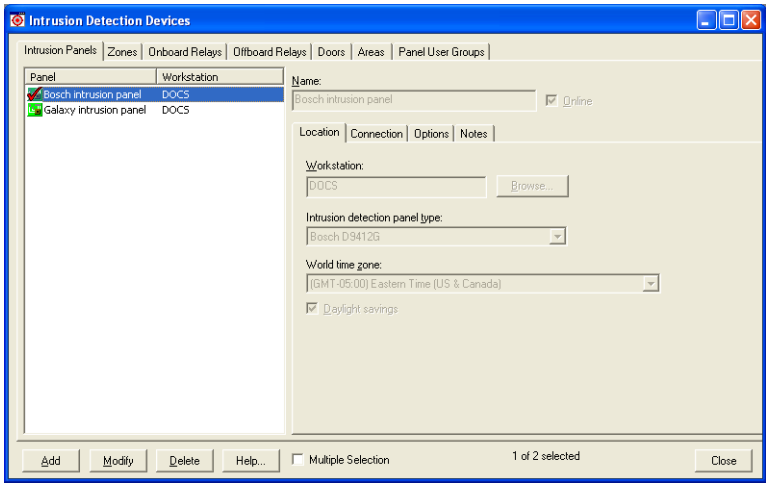
Help
Click this button to display online help for this form.

Multiple Selection
If selected, more than one intrusion panel entry in the listing window can be selected and modified or deleted simultaneously. Options that cannot be modified simultaneously will appear grayed out.

Change Segment
In modify mode, click this button to display the Segment Membership window from where you can change the selected intrusion panel’s segment.

Close
Click this button to close the Intrusion Detection Devices folder.

Intrusion Panels Form (Location Sub-tab)



Workstation

Select the workstation the intrusion panel is connected to. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/ configured.)

Browse

Opens a Browse for Computer window from which you can select a workstation.

World time zone

Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

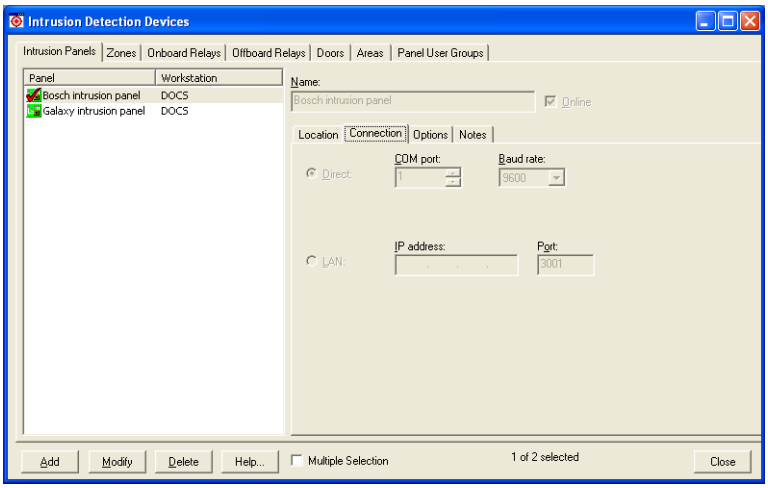
Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Intrusion detection panel type

Displays a list of intrusion detection panel types.

Intrusion Panels Form (Connection Sub-tab)



Direct

Select this radio button if workstation will communicate with the intrusion panel over a direct serial connection.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one intrusion panel. Choose a value in the range of 1 through 256.

Baud rate

If you selected the **Direct** radio button, enter the speed (in bits per second) at which information is transferred between the workstation and the intrusion panel.

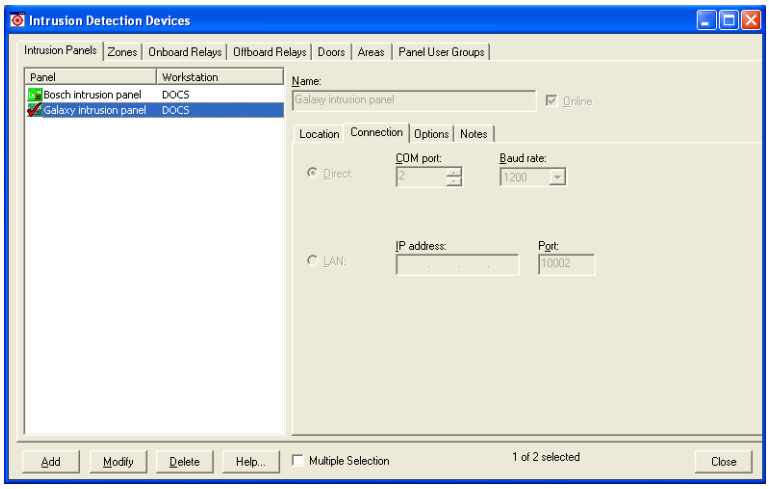
LAN

Select this radio button if the workstation will communicate with the intrusion panel over a Local Area Network. You must also specify the workstation's IP address.

IP Address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the intrusion panel, as provided by your LAN Network Administrator.

Intrusion Panels Form (Connection Sub-tab for Galaxy)

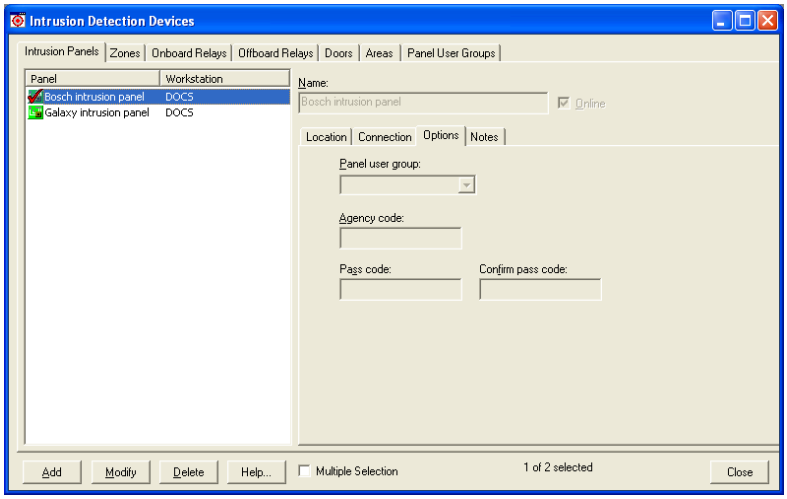


Port

Only available if a Galaxy **Intrusion detection panel type** is chosen. When configuring a Galaxy panel with a LAN connection type, a port number must be assigned. The port number must be different from other panels that are used on the same workstation.

The Port number is only utilized when configuring a Galaxy panel that is communicating using the Galaxy Ethernet module. If the Galaxy panel is using the Lantronix adapter, the port number will not be needed. The Galaxy Ethernet module is not supported for Galaxy Dimension panels. When using a Lantronix device with Galaxy Dimension panels, this port value has no effect; port 3001 is always used.

Intrusion Panels Form (Options Sub-tab)



Panel user group

Select the panel user group assigned to the panel. The panel user group is used to map the user ID in the panel to a cardholder.

Agency code

Enter the agency code for the panel. The agency code is a five digit hexadecimal code (similar to a login ID).

This field applies only to Detection Systems intrusion detection panel types.

Onboard input / output module uses line 0 addressing

For Galaxy 3-144, 3-520, and Dimension GD520 only. This must match the Dip Switch 8 setting on the panel. Unchecked, this option equals DIP Switch 8 is off. Checked, the option equals DIP Switch 8 = on.

If the **Onboard input/output module uses line 0 addressing** check box is not checked then a number of zones, onboard relays, and offboard relays will be non-configurable.

Pass code

Enter the pass code for the panel. This field applies to Detection Systems and Galaxy panel types only.

- **Detection Systems** - The pass code is a 5-digit hexadecimal code (similar to a password).
- **Galaxy** - The pass code can be up to 24 characters long.

Confirm pass code

Confirm the pass code entered in the Pass code field.

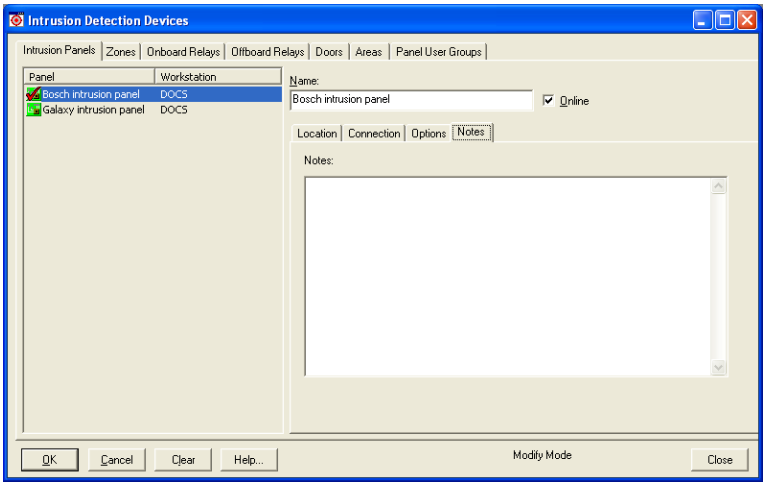
Dongle number

If using an Guardall EMEA panel, enter the dongle number. The dongle number can be any number up to 10 digits. The dongle number must also be programmed in each PX panel that will be connected to OnGuard.

Panel model

Select the panel model that is being used.

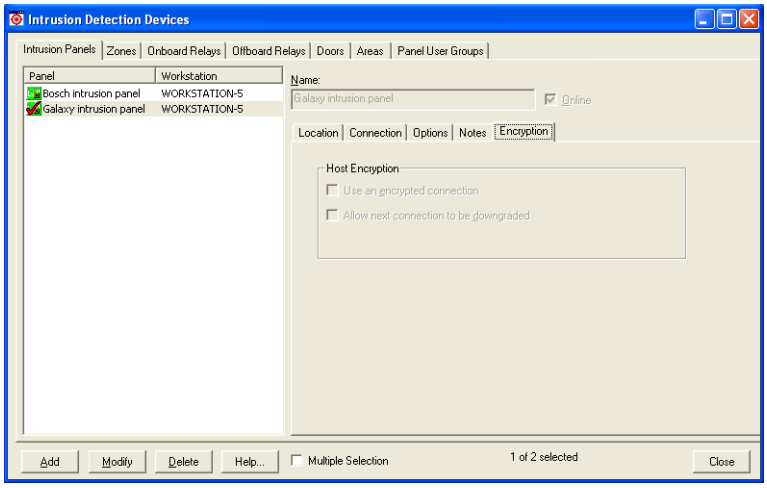
Intrusion Panels Form (Notes Sub-tab)



Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Monitor Devices chapter in the Alarm Monitoring User Guide.

Intrusion Panels Form (Encryption Sub-tab)



Note: Configuration on this tab will be disabled unless the panel is configured for a LAN connection type on the Connection sub-tab.

Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key and then by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible. This check box displays only if the controller exists in an automatic key management system/segment.

Intrusion Panels Form Procedures

Use the following procedures on this form.

Add an Intrusion Panel

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***. The Intrusion Detection Configuration folder opens.
2. On the Intrusion Panels tab, click [Add].
3. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this intrusion panel will be assigned to.
   b. Click [OK].
4. In the **Name** field, type an intrusion panel name. Intrusion panel names can be up to 32 characters.
5. Select whether the receiver is online or offline.When an intrusion panel is online, the Communication Server attempts to communicate with the device.
6. On the Location sub-tab:
   a. Select the **Workstation** to which the intrusion panel is connected to. The Communication Server must be running on the specified workstation.
   b. Select the world time zone from the **World time zone** drop-down list.
   c. Select whether **Daylight savings** is used or not.

Note: The workstation name is obtained from Microsoft Windows by right-clicking the My Computer desktop icon and selecting **Properties**. The workstation name is located on the Computer Name tab.

7. Select an intrusion panel type that is valid for the installed software license.
8. Click the Connection sub-tab.
9. Select the method that will be used to communicate with the intrusion panel.
   - Select the **Direct** radio button if the workstation will communicate with the intrusion panel through a direct serial connection. You must also specify the workstation's COM port and baud rate.

     IMPORTANT: Bosch panels (DS7400Xi Version 3+ and 4+) both have 2400 and 9600 baud rates, with 2400 being the default. Bosch panels (D7412 and D9412) have a fixed baud rate of 9600. Galaxy default baud rate is 1200 and supports baud rates of 1200, 2400, 4800, 9600, 19200, and 38400.

   - Select the **LAN** radio button if the workstation will communicate with the intrusion panel through a Local Area Network. You must also specify the panel or Lantronix IP address.
10. Click the Options sub-tab.

11. Select the **Panel user group** assigned to the panel. The panel user group is used to map the user ID in the panel to a cardholder. For more information, refer to Add a Panel User Group on page 1146.
12. Bosch only - require the Agency and Pass code. These fields are automatically populated with default values when you click [OK]. It is recommended you use the default values.

    Galaxy is capable of a Pass code but it is not required. If the panel has been configured with a pass code then the pass code entered must matched the pass code in the panel in order to communicate with the panel. Configure the Galaxy panel pass code using the Ademco Galaxy Gold software application.

    Galaxy 3-144, 3-520, and Dimension GD520 only: Check or uncheck the **Onboard input/output module uses line 0 addressing** check box. This much match the Dip Switch 8 setting on the panel. Unchecked, this option equals DIP Switch 8 is off. Checked, the option equals DIP Switch 8 = on.

    - If the **Onboard input/output module uses line 0 addressing** check box is not checked then a number of zones, onboard relays, and offboard relays will be non-configurable.

Note: The agency and pass code are five digit hexadecimal codes (similar to a login ID) used by the LS Communication server. For Galaxy panels the pass code can include any characters and be 24 characters long.

13. Click [OK].

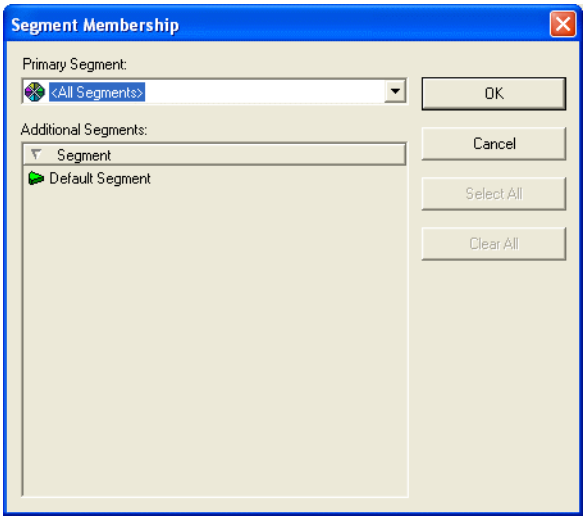
Modify an Intrusion Panel

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. On the Intrusion Panels tab, select the entry you want to modify. If the **Multiple Selection** check box is selected, you can select more than one intrusion panel entry.
3. Click [Modify].
4. Make any desired changes.
5. Click [OK].
6. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

Modify an Intrusion Panel's Segment

Note: This procedure applies only to segmented systems.

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Intrusion Panels tab.
3. Select (place a checkmark beside) the entry you want to modify.
4. Click [Modify].
5. Click [Change Segment]. The Segment Membership window opens.
6. Select a segment to move the intrusion panel to.



7. Click [OK].

Delete an Intrusion Panel

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. On the Intrusion Panels tab, select the entry you want to delete. If the **Multiple Selection** check box is selected, you can select more than one intrusion panel entry.
3. Click [Delete].
4. Click [OK].
5. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

Enable an Intrusion Panel for Encryption

The encryption modify/export permission is required to complete this procedure. Also, encryption must be enabled and the proper encryption key configured in the communication device before enabling the panel for encryption.

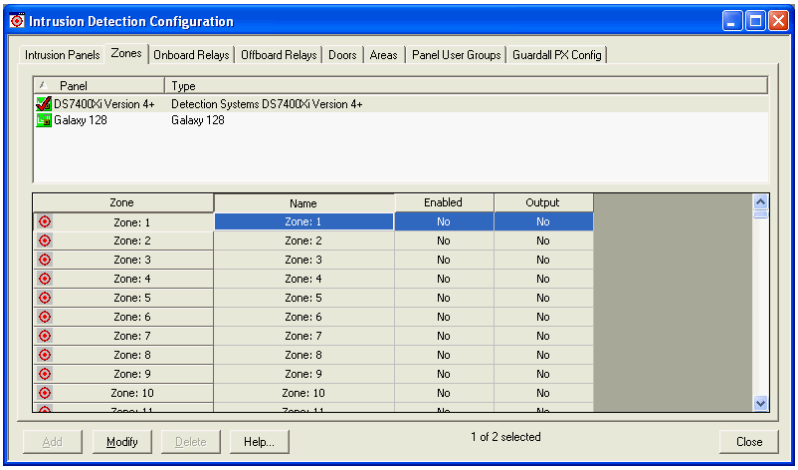
1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. On the Intrusion Panels form, click the Encryption sub-tab.
3. In the listing window, select the Intrusion Panels entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Enter Notes for a Panel

1. In the listing window, select the entry you want to edit.
2. Click [Modify].

3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

Zones Form



Note: The information displayed in the **Zone** and **Name** columns depends on the type of panel selected.

Listing window

Lists currently defined intrusion panels. A icon precedes each entry.

Zone

Displays the pre-configured intrusion zone names.This field cannot be changed.

Name

Displays the user-configured intrusion zone names. Each name can be up to 64 characters long. The zone must be enabled before you can save changes to the zone name.

Enabled

Indicates if the zone name is enabled or disabled. If enabled, the user-configured zone name displays in Alarm Monitoring. If disabled, the pre-configured zone name displays in Alarm Monitoring.

Output

Indicates if the zone is being used as an output. This field applies only to Detection Systems intrusion detection panel types.

Add

This button is not used.

Modify

Click this button to configure intrusion zones.

Delete
This button is not used.

Help
Click this button to display online help for this form.

Close
Click this button to close the Intrusion Detection Devices folder.

Maximum Number of Zones

A zone is an input to a panel and is sometimes referred to as a point (e.g. smoke detector or motion detector). The number of zones you can configure per panel depends on the panel type. Refer to the following table.

Zones per panel	Panel type
128	Bosch DS7400Xi Version 3+
248	Bosch DS7400Xi Version 4+
75	Bosch D7412
246	Bosch D9412
8	Galaxy 8
18	Galaxy 18
48	Galaxy 3-48
60	Galaxy 60
128	Galaxy 128
144	Galaxy 3-144
504	Galaxy 500
512	Galaxy 504 and 512
520	Galaxy 3-520
48	Galaxy Dimension GD48
520	Galaxy Dimension GD520

Zones Form Procedures

Intrusion detection zones are configured in both Bosch software and Lenel software (OnGuard). Configuring intrusion detection zones in OnGuard allows you to view the zones in the Alarm Monitoring system hardware tree as well as view zone names (instead of the Bosch zone number) when the zone is in alarm.

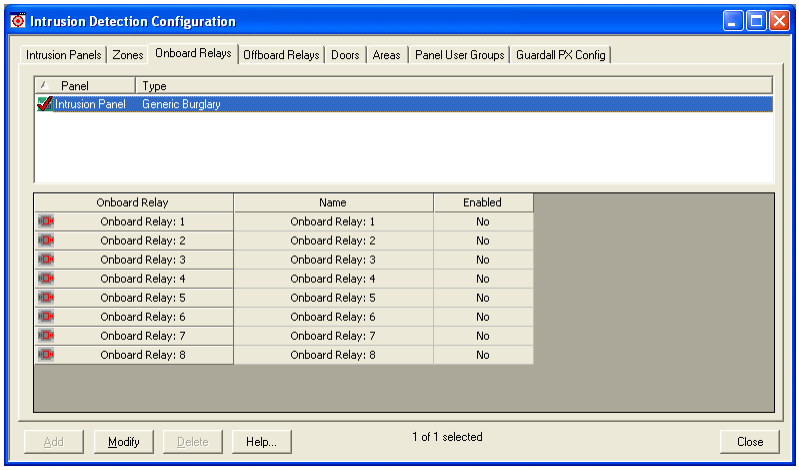
Configure Intrusion Zones

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Zones tab.
3. Select the intrusion panel that you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the **Name** column to activate the field. A cursor appears in the active field. Enter the name of this intrusion zone.
   b. Double-click the **Enabled** cell to toggle between Yes (enabled) and No (disabled). If you enable the zone, its name appears (instead of its Bosch configured number) in Alarm Monitoring when the zone is in alarm.
   c. Bosch Systems only. Double-click the **Output** cell to toggle between Yes and No. Yes indicates the zone is an output zone and has hardware associated with it. No indicates the zone is an input.

Note: If the zone is an output zone then you can activate the output from Alarm Monitoring.

   d. Repeat step 5 for each zone you want to configure.
6. Click [OK].

Onboard Relays Form



Note: The information displayed in the **Onboard Relay** and **Name** columns depends on the type of panel selected.

Listing window

Lists currently defined intrusion panels. A icon precedes each entry.

Onboard Relay

Displays the pre-configured onboard relay names.This field cannot be changed.

Name
Displays the user-configured onboard relay names. Each name can be up to 64 characters long. The onboard relay must be enabled before you can save changes to the relay name.

Enabled
Indicates if the relay name is enabled or disabled. If enabled, the user-configured relay name displays in Alarm Monitoring. If disabled, the pre-configured relay name displays in Alarm Monitoring.

Add
This button is not used.

Modify
Click this button to configure onboard relays.

Delete
This button is not used.

Help
Click this button to display online help for this form.

Close
Click this button to close the Intrusion Detection Devices folder.

Maximum Number of Onboard Relays

The number of relays you can configure per panel depends on the panel type. Refer to the following table.

Onboard relays per panel	Panel type
5	Bosch DS7400Xi Version 3+
5	Bosch DS7400Xi Version 4+
3	Bosch D7412
3	Bosch D9412
6	Galaxy 8, 18, and 60
4	Galaxy 128, 500, 504, and 512
8	Galaxy 3-48, 3-144, 3-520
8	Galaxy Dimension GD48
12	Galaxy Dimension GD520

Onboard Relays Form Procedures

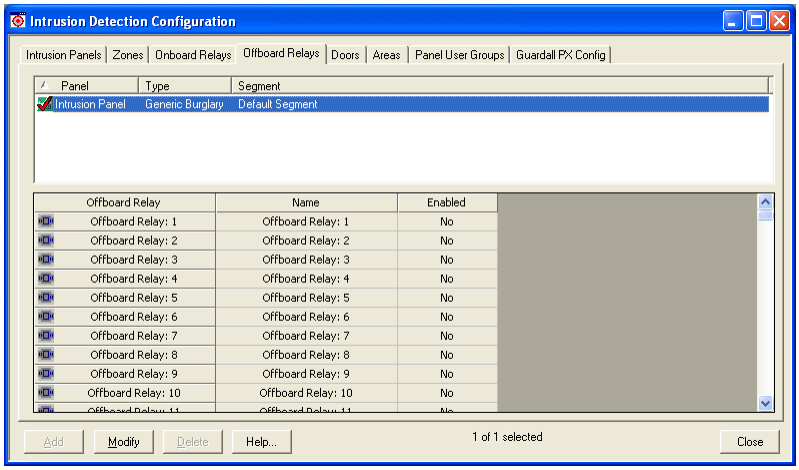
Onboard relays are configured in both Bosch software and Lenel software (OnGuard). Configuring onboard relays in OnGuard allows you to view the relay in the Alarm Monitoring system hardware

tree as well as view relay names (instead of the Bosch relay number) when the onboard relay is in alarm.

Configure Onboard Relays

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Onboard Relays tab.
3. Select the intrusion panel you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the **Name** column to activate the field. A cursor appears in the active field. Enter the name of this onboard relay.
   b. Double-click the **Enabled** cell to toggle between Yes (enabled) and No (disabled). If you enable the relay, its name appears (instead of its Bosch configured letter) in Alarm Monitoring when the relay is in alarm.
6. Repeat step 5 for each relay that you want to configure.
7. Click [OK]

Offboard Relays Form



Note: The information displayed in the **Offboard Relay** and **Name** columns depends on the type of panel selected.

Listing window

Lists currently defined intrusion panels. A icon precedes each entry.

Offboard Relay

Displays the pre-configured offboard relay names.This field cannot be changed.

Name

Displays the user-configured offboard relay names. Each name can be up to 64 characters long. The offboard relay must be enabled before you can save changes to the relay name.

Enabled
Indicates if the relay name is enabled or disabled. If enabled, the user-configured relay name displays in Alarm Monitoring. If disabled, the pre-configured relay name displays in Alarm Monitoring.

Add
This button is not used.

Modify
Click this button to configure offboard relays.

Delete
This button is not used.

Help
Click this button to display online help for this form.

Close
Click this button to close the Intrusion Detection Devices folder.

Maximum Number of Offboard Relays

The number of relays you can configure per panel depends on the panel type. Refer to the following table.

Offboard relays per panel	Panel type
16	Bosch DS7400Xi Version 3+, Bosch Bosch DS7400Xi Version 4+
64	Bosch D7412
128	Bosch D9412
0	Galaxy 8
3	Galaxy 18
4	Galaxy 60, Galaxy 3-48
8	Galaxy 128, Galaxy 3-144
16	Galaxy 500
32	Galaxy 504, 512
252	Galaxy 3-520
16	Galaxy Dimension GD48
252	Galaxy Dimension GD520

Offboard Relays Form Procedures

Offboard relays are configured in both Bosch software and Lenel software (OnGuard). Configuring offboard relays in OnGuard allows you to view the relay in the Alarm Monitoring system hardware tree as well as view relay names (instead of the Bosch relay number) when the offboard relay is in alarm.

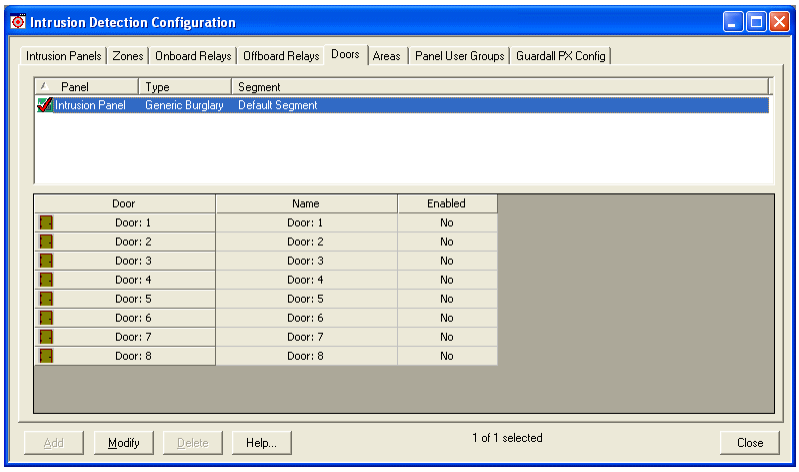
Configure Offboard Relays

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Offboard Relays tab.
3. Select the intrusion panel you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the **Name** column to activate the field. A cursor appears in the active field. Enter the offboard relay name.
   b. Double-click the **Enabled** cell to toggle between Yes (enabled) and No (disabled). If you enable the relay, its name appears in Alarm Monitoring instead of its pre-configured relay name.
6. Repeat step 5 for each relay that you want to configure.
7. Click [OK].

Doors Form

The Doors form applies to Generic and Bosch devices only. You can configure up to eight (8) doors with Generic and Bosch 9412 devices, and up to two (2) doors with Bosch 7412 devices.

Note: The Door Control Module (DCM) for Galaxy Dimension panels is not supported.



Listing window

Lists currently defined intrusion panels. A icon precedes each entry

Door
Displays the pre-configured door names. This field cannot be changed.

Name
Displays the user-configured door names. Each name can be up to 64 characters long. The door must be enabled before you can save changes to the door name.

Enabled
Indicates if the door name is enabled or disabled. If enabled, the user-configured door name displays in Alarm Monitoring. If disabled, the pre-configured door name displays in Alarm Monitoring.

Add
This button is not used.

Modify
Click this button to configure a door.

Delete
This button is not used.

Help
Click this button to display online help for this form.

Close
Click this button to close the Intrusion Detection Devices folder.

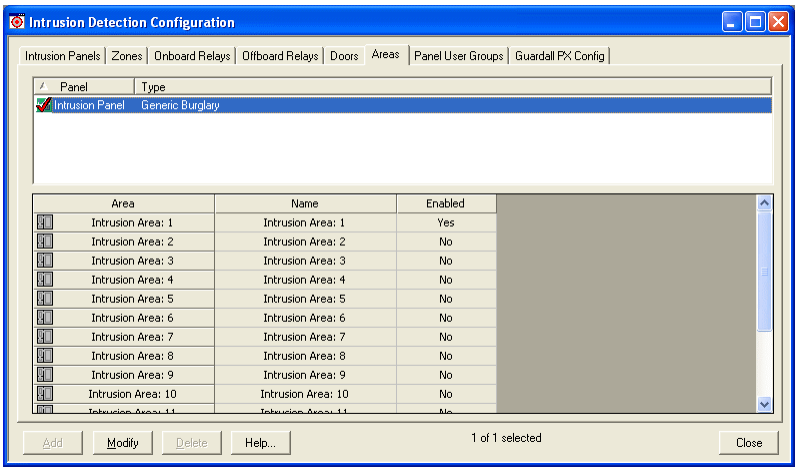
Doors Form Procedures

Intrusion detection doors are configured in both RAM IV software and Lenel software (OnGuard). Configuring doors in OnGuard allows you to view the door in the Alarm Monitoring system hardware tree as well as view the name of the door (instead of its Bosch number) when the door is in alarm.

Configure Intrusion Doors

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Doors tab.
3. Select the intrusion panel you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the **Name** column to activate the field. A cursor appears in the active field. Enter the intrusion door name.
   b. Double-click the **Enabled** cell to toggle between Yes (enabled) and No (disabled). If you enable the door, its user-configured name appears in Alarm Monitoring instead of its pre-configured door name.
6. Repeat step 5 for each intrusion door that you want to configure.
7. Click [OK].

Areas Form



Listing window

Lists currently defined intrusion panels. A icon precedes each entry.

Area

Displays the pre-configured intrusion area names. This field cannot be changed.

Name

Displays the user-configured intrusion area names. Each name can be up to 64 characters long. The area must be enabled before you can save changes to the area name.

Enabled

Indicates if the area name is enabled or disabled. If enabled, the user-configured area name displays in Alarm Monitoring. If disabled, the pre-configured area name displays in Alarm Monitoring.

Add

This button is not used.

Modify

Click this button to configure an intrusion area.

Delete

This button is not used.

Help

Click this button to display online help for this form.

Close

Click this button to close the Intrusion Detection Devices folder.

Maximum Number of Areas

An area is a separately configurable section of the panel, referred to as partitions in Detection Systems and Bosch panels. Areas can have multiple zones assigned to them. The number of configurable areas available depend on the panel type. Refer to the following table.

Areas per panel	Panel type
8	Bosch DS7400Xi Version 3+
8	Bosch DS7400Xi Version 4+
8	Bosch D7412
8	Bosch D9412
0	Galaxy 8
3	Galaxy 18
4	Galaxy 60, 3-48
8	Galaxy 128, 3-144
16	Galaxy 500
32	Galaxy 54, 512, 3-520
8	Galaxy Dimension GD48
32	Galaxy Dimension GD520

Areas Form Procedures

Use the following procedures on this form.

Configure an Area

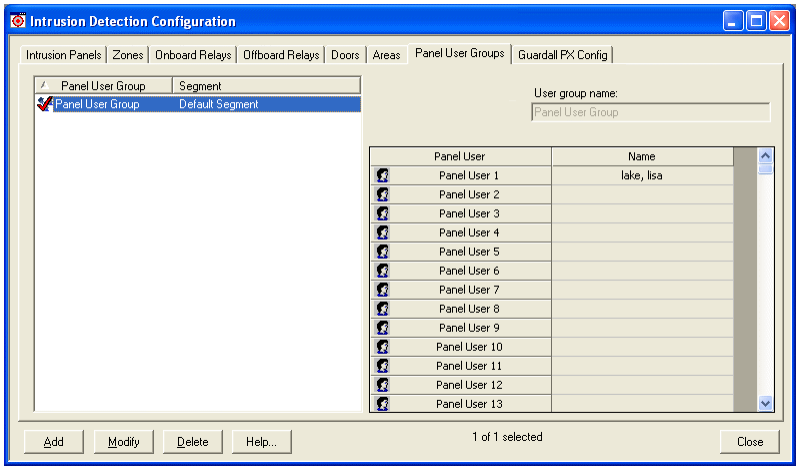
Intrusion detection areas are configured in both Bosch software and Lenel software (OnGuard). Configuring areas in OnGuard allows you to view the area in the Alarm Monitoring system hardware tree as well as view area names (instead of the Bosch area number) when the area is in alarm.

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Areas tab.
3. Select the intrusion panel that you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the **Name** column to activate the field. A cursor appears in the active field. Enter the name of the intrusion area. Each name can contain no more than 64 characters.
   b. Double-click the **Enabled** cell to toggle between Yes (enabled) and No (disabled). If you enable the area, its name appears (instead of its Bosch configured number) in Alarm Monitoring when the area is in alarm.
6. Repeat step 5 for each intrusion area that you want to configure.

7. Click [OK].

Panel User Groups Form

The Panel User Groups link cardholders to user events. OnGuard cardholders can be assigned to panel user groups. Each panel user group can store up to 1000 panel users. Detection Systems and Bosch support up to 300 panel users; Galaxy supports up to 1000 panel users.



Listing window

Lists currently defined panel user groups. A icon precedes each entry.

User group name

Identifies the name of the panel user group. This is a “friendly” name assigned to each panel user group to make it easy to identify. Each name can be up to 64 characters long.

Panel User

Displays the default description of the panel user.

Name

Identifies the name of the cardholder that is linked to the panel user.

Add

Click this button to add a panel user group.

Modify

Click this button to modify a panel user group.

Delete

Click this button to delete a panel user group.

Help

Click this button to display online help for this form.

Change Segment

In modify mode, click this button to display the Segment Membership window from where you can change the selected panel user group's segment.

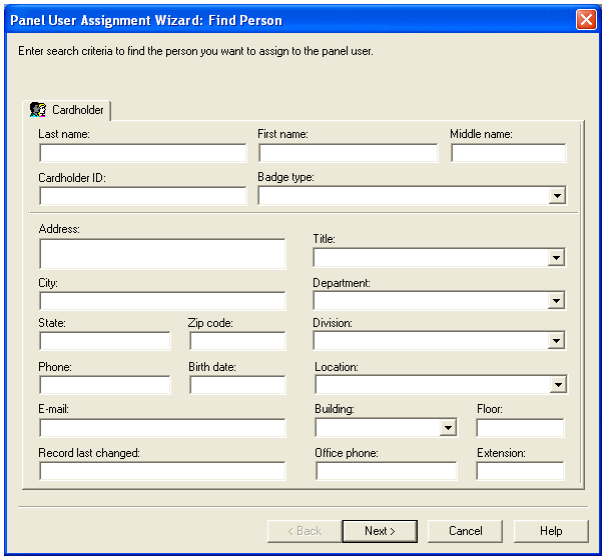
Close

Click this button to close the Intrusion Detection Devices folder.

Panel User Assignment Wizard: Find Person Form

Note: If the FormsDesigner application has been used to customize your cardholder data, the elements on your Panel User Assignment Wizard: Find Person form will be different. The default fields are pictured in the following graphic.

This form is displayed when you double-click on a cell in the **Name** column in the table on the Panel User Groups form in add or modify mode.



Last name

Indicates cardholder's last name.

First name

Indicates cardholder's first name.

Middle name

Indicates cardholder's middle initial.

Cardholder ID

Indicates cardholder's ID number.

Badge type

Selects which of the cardholder's badges (if he or she has more than one) is to be the active one.

User-defined fields

All fields below the Cardholder ID and Badge type fields are considered user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your cardholder data.

Back

This button is not used.

Next

When clicked:

- If the system locates more than one record matching your search criteria, the wizard will proceed to the Panel User Assignment Wizard: Select Person form.
- If the system locates only one record matching your search criteria, the wizard will proceed to the Panel User Assignment Wizard: Summary form.

Cancel

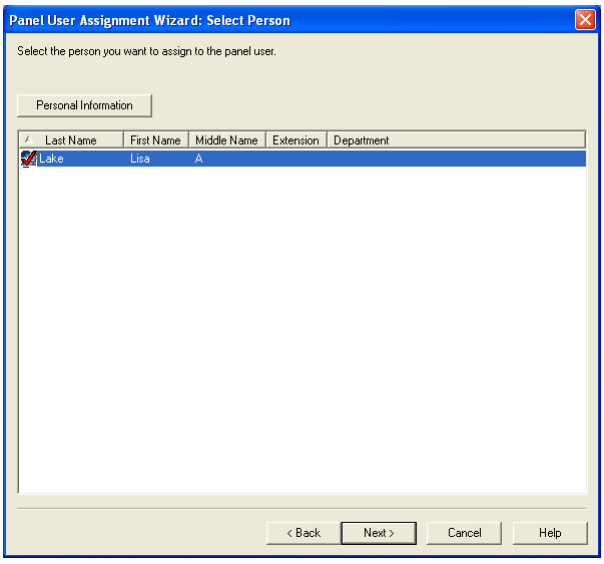
Click this button to close the wizard and return to the Panel User Groups form.

Help

Click this button to display online help for this form.

Panel User Assignment Wizard: Select Person Form

This form is displayed when you click the [Next] button on the Panel User Assignment Wizard: Find Person form and the system locates more than one record matching your search criteria.



Panel User Assignment Wizard: Select Person Form

Personal Information

Click this button to display information on the cardholder selected in the listing window.

Listing window

Lists all cardholder records that match the search criteria that you entered on the Panel User Assignment Wizard: Find Person form.

Back

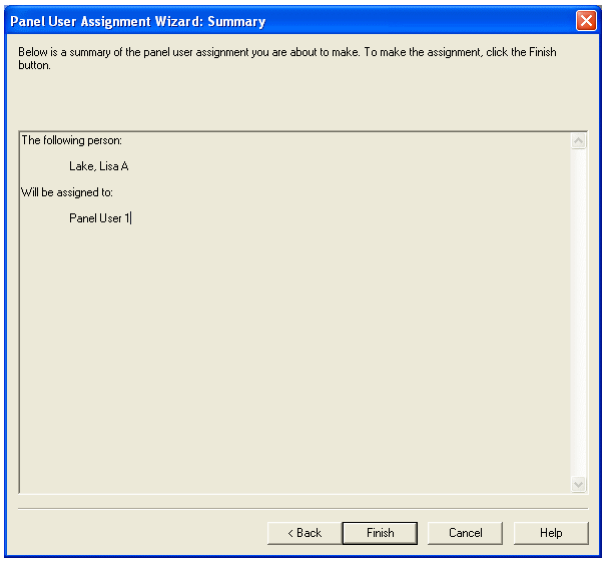
Click this button to return to the Panel User Assignment Wizard: Find Person form.

Next

When you select a cardholder in the listing window and clicks this button, the wizard proceeds to the Panel User Assignment Wizard: Summary form.

Panel User Assignment Wizard: Summary Form

This form is displayed when you click the [Next] button on the Panel User Assignment Wizard: Find Person form and the system locates only one record matching your search criteria or when you click the [Next] button on the Panel User Assignment Wizard: Select Person form.



Summary window

Displays a summary of the panel user assignment that you are about to make.

Back

Click this button to return to the Panel User Assignment Wizard: Select Person form.

Finish

Click this button to make the assignment displayed in the summary window.

Panel User Groups Form Procedures

Use the following procedures on this form.

Add a Panel User Group

The Panel User Groups link cardholders to user events.

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Panel User Groups tab.
3. Click [Add].
4. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this panel user group will be assigned to.
   b. Click [OK].
5. In the **User group name** field, type a name for the panel user group.
6. In the table located on the right half of the form, double-click a panel user.
7. The Panel User Assignment Wizard: Find Person window opens.
8. Specify your search criteria by typing full or partial entries in the fields. For more information, refer to Panel User Assignment Wizard: Find Person Form on page 1143.
9. Click [Next]. One of the following happens:
   - If the system locates only one cardholder record based on your search criteria, the Panel User Assignment Wizard: Summary form opens.
   - If the system locates more than one cardholder record matching your search criteria, the Panel User Assignment Wizard: Select Person window opens.
     i. Select a cardholder from the listing window.
     ii. Click [Personal] to display information on the selected cardholder. Click [OK] to return to the Wizard.
     iii. Click [Next]. The Panel User Assignment Wizard: Summary form opens.
10. Click [Finish] to make the assignment display in the summary window.
11. Repeat steps 6 - 10 for each panel user name you want to configure.
12. Click [OK].

Modify a Panel User Group

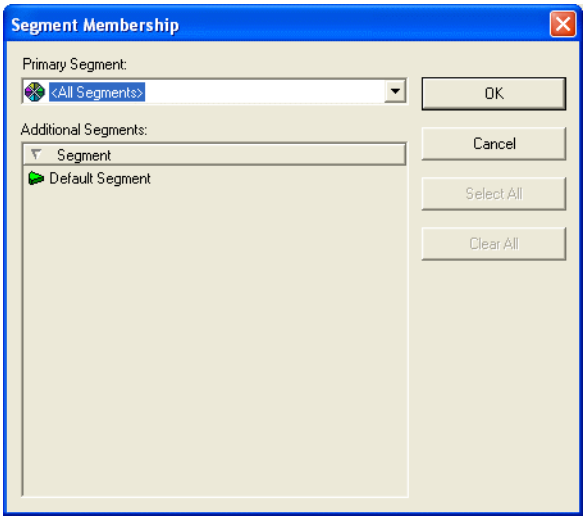
1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Panel User Groups tab.
3. Click the panel user group entry you want to modify from the listing window to select it.
4. Click [Modify].
5. Make any desired changes.
6. Click [OK].
7. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

Modify a Panel User Group's Segment

Note: This procedure applies only to segmented systems.

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Panel User Groups tab.
3. Click the panel user group entry you want to modify from the listing window to select it.
4. Click [Modify].

5. Click [Change Segment]. The Segment Membership window opens.



6. Select a segment to move the panel user group to.
7. Click [OK].

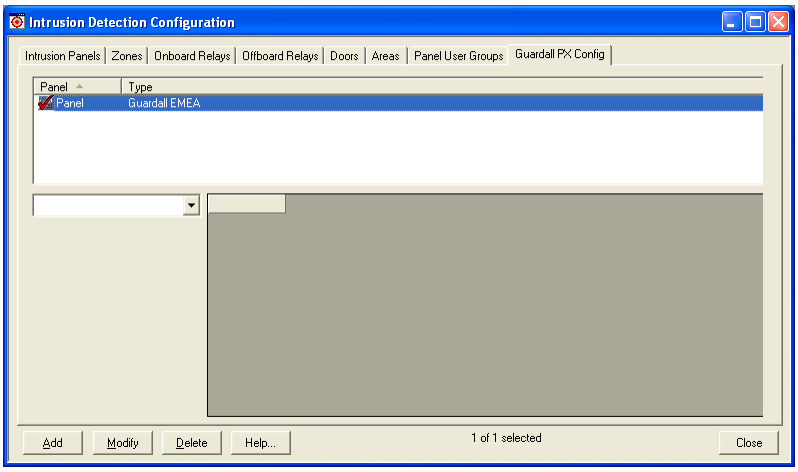
Delete a Panel User Group

A panel user group cannot be deleted if it is currently assigned to one or more intrusion panels.

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Panel User Groups tab.
3. Click the panel user group entry you want to delete from the listing window to select it.
4. Click [Delete].
5. Click [OK].
6. A prompt to confirm that you want to make the deletion will be displayed. Click [Yes].

Guardall PX Config Form

The Guardall PX Config form allows Guardall EMEA panels to interface with the OnGuard software. All panel versions from v4.01 are supported. The panel connection to OnGuard can be Ethernet, Serial or Modem. Your OnGuard license must support Intrusion Detection devices.



Listing window

Lists currently defined panels.

Drop-down box

Select PX panel options from the drop-down box. Selecting different options allows you change different system options.

Panel

Displays the default description of the panel.

PX Integration Procedures

For more information, refer to PX Panel Integration on page 1589.

CHAPTER 57

POS Devices Folder

The POS (Point of Sale) Devices folder contains forms with which you can:

- Configure POS devices to communicate with the OnGuard software.
- Associate multiple registers with a POS device.

The POS Devices folder contains the POS Devices and POS Register form.

This folder is displayed by selecting ***POS Devices*** from the ***Additional Hardware***, or selecting the POS Devices toolbar button.

Toolbar Shortcut

POS Devices Overview

POS devices, also known as video text inserters or cash register/point of sale video interfaces, are used in conjunction with video devices to monitor transactions at cash registers and ATM machines. POS devices translate transactions into events or activity alarms. Although they can also superimpose transaction information (insert text) directly onto corresponding video, OnGuard does not currently support this.

Using OnGuard with POS Devices

You can configure OnGuard to receive cash register transactions (events) from POS devices and store individual transactions in a database. Furthermore, the ability to associate video cameras with hardware devices and couple hardware events with digital video clips, extends to POS devices. For example, when an item is voided or an employee signs on to a register, you can configure OnGuard to record video at that register and generate an alarm in Alarm Monitoring.

The procedures you would follow to link POS devices to a camera, generate alarms, record and lock video events have not changed.

Hardware Setup and Configuration

In order for OnGuard to receive events from cash register transactions, you must connect each register to a POS device and then connect the POS device to the OnGuard workstation. Currently, OnGuard supports the **TVC-2100 Series** POS device which interfaces with up to 10 registers.

The POS device is configured in System Administration through the POS Devices folder. To configure the POS device, you identify the OnGuard workstation it connects to and the mode of communication it uses (direct or LAN). To differentiate events between registers, each register is assigned a number in the OnGuard software. The register number must match the number reported to the database during transactions.

Note: For hardware installation information refer to the Hardware Installation User Guide.

Storing Transactions

OnGuard stores every transaction separately. For example, the sale of individual items, calculating the tax for a bill and calculating the total bill are considered separate transactions. If a person purchases a carton of eggs and a gallon of milk, five transactions are recorded:

1. Eggs $1.55
2. Milk $1.98
3. Subtotal $3.53
4. Tax $0.25
5. Total $3.78

The data returned in each transaction includes the register number, a description of the register activity, an action code that identifies the item purchased, the quantity purchased and dollar amount.

Licenses Required

Two types of license options are required to use POS devices. The “Maximum Number of Points of Sale Registers” license is for the number of registers you plan to use. The “Maximum Number of Point of Sale Devices (SWG-1380)” is based on the POS device. These license options are listed in License Administration under Access Control Options. Licenses are based, not on the type of controller, but instead the number of controllers for a given panel class.

User Permissions Required

User permissions are required to add, modify and delete POS devices. The permissions are set on the Additional Data Sources sub-tab of the System Permission Groups form.

In addition, user permissions are required to trace POS devices in Alarm Monitoring. This permission is set in System Administration on the Monitor sub-tab of the Monitor Permission Groups form.

POS Devices Folder

The following table lists the fields found on every form and sub-tab in the POS Devices folder.

POS Devices Folder - Common Fields

Add
Adds a POS device or register.

Modify
Changes the settings of a selected POS device or register.

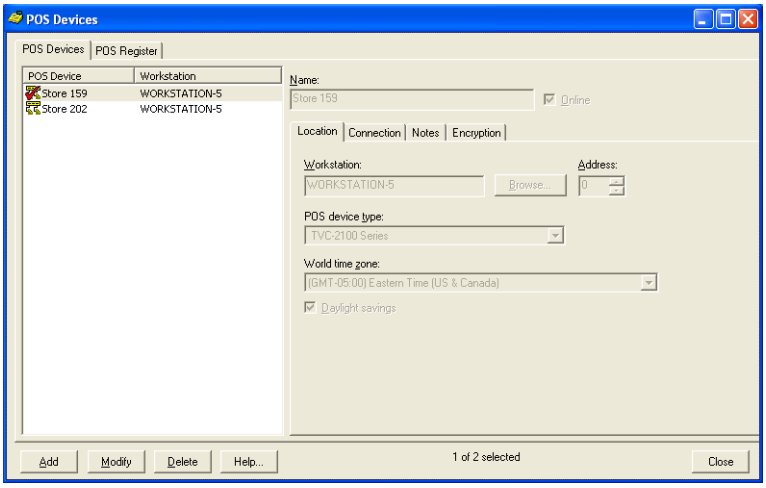
Delete
Deletes the selected POS device or register.

Help
Displays online help for this form.

Close
Closes the POS Devices folder.

POS Devices Form (Location Sub-tab)

The POS Devices form enables a POS device to communicate with the OnGuard software. The Location sub-tab identifies the workstation that will receive events from the POS device.



Listing Window
Displays POS devices and the workstations associated with them.

Name
A descriptive name of the POS device.

Online
Places the POS device online.

Workstation
The workstation POS device connects to in order to transfer events. The Communication Server must be present of the specified workstation. You can either enter the workstation name or browse

the workstations available on the network. You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse
Displays a Browse for Computer window from which you can select a workstation.

Address
The POS device box number.

POS device type
Select the POS device type.

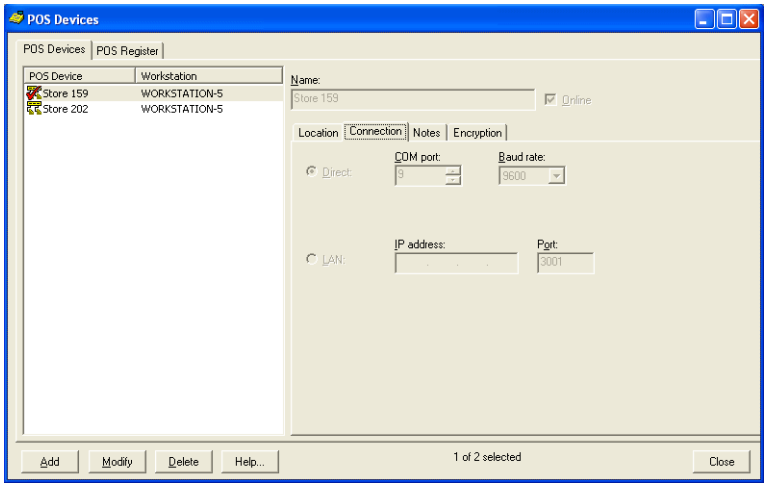
World time zone
Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings
Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

POS Devices Form (Connection Sub-tab)

The Connection sub-tab identifies the mode of communication as either direct or over the network.



Direct
Identifies the mode of communication between the POS device and the workstation as being direct.

COM port
The COM port used to connect the POS device to the workstation, if the mode of communication is direct.

Baud rate

The baud rate is the rate (in bits per second) at which data is transferred from the POS device to the workstation, if the mode of communication is direct.

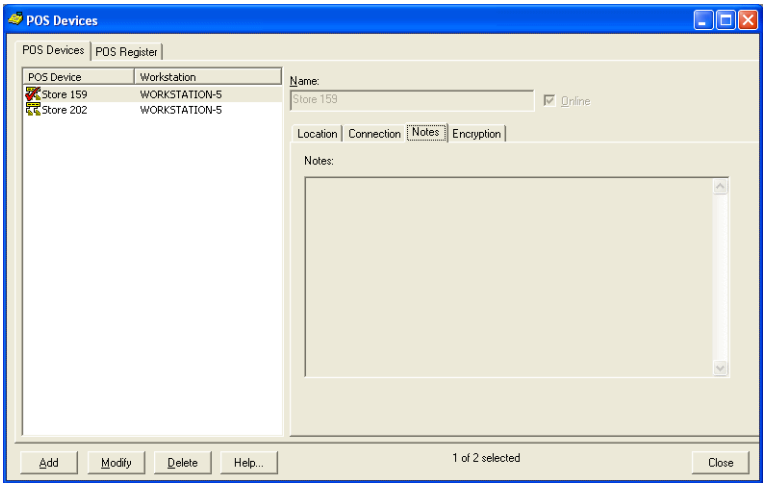
LAN

Identifies the mode of communication between the POS device and the workstation as being through the internet.

IP address

The Internet Protocol (TCP/IP) address for the POS device. The POS device itself must be configured to have the same IP address as what you enter in this field.

POS Devices Form (Notes Sub-tab)



Notes

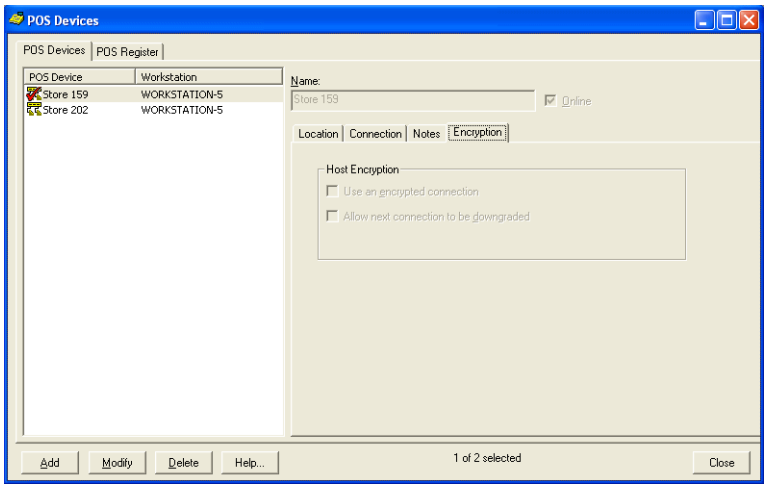
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered shere will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

POS Devices Form (Encryption Sub-tab)

This view displays when the system/segment (the panel is associated with) uses automatic encryption. The same fields display when the system/segment is configured for manual encryption, except for the **Allow next connection to be downgraded** check box.The Encryption sub-tab does not display if a system/segment uses a plain connection.

Note: The system/segment the controller belongs to must be configured for encryption in order for this tab to display. This tab will be disabled unless the panel is configured for a LAN connection type on the Connection sub-tab. The user must also have the correct user permissions.

For more information about encryption, refer to the Encryption for Controllers User Guide.



Use an encrypted connection

Determines whether the connection to the controller is encrypted or not. If not selected (the default), a plain connection is used. If selected, the connection is encrypted.

Allow next connection to be downgraded

Determines whether the system will attempt a downgrade the next time it connects to the controller and there are encryption problems. If not selected (the default), the system will not attempt to downgrade the connection, even if the configured encrypted connection fails. If selected, the system will attempt to downgrade the connection if the encrypted connection fails.

The system attempts downgrades by trying encryption with the inactive master key and then by trying a plain connection. Note that if the controller requires encryption, a plain connection is not possible. This check box displays only if the controller exists in an automatic key management system/segment.

POS Devices Form Procedures

Use the following procedures on this form.

Configure a POS Device

1. From the ***Additional Hardware*** menu, select ***POS Devices***.
2. The POS Devices form opens. Click [Add].
3. Enter a descriptive name for the POS device and select the **Online** check box.
4. On the Location sub-tab:
   - Enter the workstation the POS device connects to.
   - Enter the POS device box number in the **Address** field.
   - Select the POS device type.
   - Select the world time zone from the **World time zone** drop-down list.
   - Select whether **Daylight savings** is used or not.
5. On the Connection sub-tab, complete one of the following:
   - Select the **Direct** radio button and enter the COM port and baud rate.
   - Select the **LAN** radio button and enter the IP address.

6. Click [OK].

Enable a POS Device for Encryption

The encryption modify/export permission is required to complete this procedure. Also, encryption must be enabled and the proper encryption key configured in the communication device before enabling the panel for encryption.

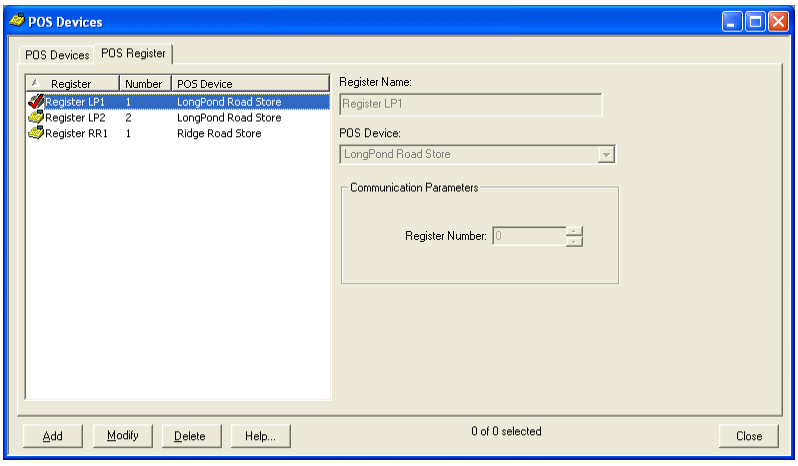
1. From the ***Additional Hardware*** menu, select ***POS Devices***.
2. On the POS Devices form, click the Encryption sub-tab.
3. In the listing window, select the POS Device entry you wish to enable encryption for.
4. Click [Modify].
5. Select the **Use an encrypted connection** check box.
6. If automatic encryption is used, you can also select the **Allow next connection to be downgraded** check box, if you want the connection downgraded if the encrypted connection fails.
7. Click [OK].
8. Acknowledge any messages that display.

Enter Notes for a POS Device

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

POS Register Form

The POS Register form is used to identify the registers associated with the POS device.



Listing Window

Displays previously configured registers, their number and the POS devices associated with them.

Register Name
A descriptive name of the register.

POS Device
The POS device that is connected to the specified register.

Register Number
The register number enables OnGuard to differentiate events received from the POS devices, since several registers are connected to the same POS device. The register number must match the number reported to the database during transactions.

POS Register Form Procedures

Use the following procedures on this form.

Associate a POS Register with a POS Device

The register name must be unique even if you are working with registers connected to different POS devices. However, you can have the same register number assigned to different registers, as long as the registers are associated with different POS devices.

1. Select ***POS Devices*** from the ***Additional Hardware*** menu. The POS Devices folder opens.
2. Click the POS Register tab.
3. On the POS Register form, click [Add].
4. Enter a descriptive name for the POS register.
5. Select the POS device connected to the register.
6. Select or enter a register number.
7. Click [OK].

CHAPTER 58

SNMP Managers Folder

The SNMP Managers folder contains forms with which you can:

- Add, modify, or delete SNMP Managers
- Add, modify, or delete SNMP Agents
- Load MIB files into OnGuard
- Modify SNMP Management Information Base variables

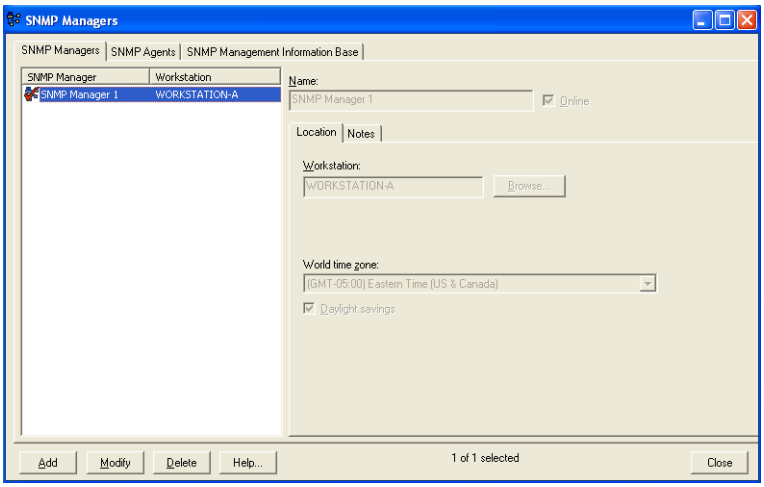
The SNMP Managers folder contains the SNMP Managers, SNMP Agents, and SNMP Management Information Base forms.

Before SNMP can be configured in OnGuard, the Windows SNMP components must be installed. Instructions for installing the Windows SNMP components, as well as additional information about SNMP can be found in the "Using SNMP with OnGuard" chapter in the Advanced Installation Topics guide.

This folder is displayed by selecting ***SNMP Managers*** from the ***Additional Hardware*** menu, or by selecting the SNMP Managers toolbar button.

Toolbar Shortcut

SNMP Managers Form (Location Sub-tab)



Listing window

Lists the name and workstation for each configured SNMP Manager.

Name

Identifies the name of the SNMP Manager. This is a “friendly” name assigned to each SNMP Manager to make it easy to identify.

Online

If selected, the SNMP Manager is online and ready for use. If deselected, the SNMP Manager is not ready for use.

Workstation

Identifies the workstation that SNMP Manager is or will be running on in order to receive events. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Brings up a list of all workstations. Whichever workstation is selected will have an SNMP Manager running on it (provided that the Online check box is selected and the Communication Server is running on it). There can only be one SNMP Manager per Communication Server.

World time zone

Select the world time zone for the selected access panel’s geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone’s clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Savings Time is enforced in the selected access panel’s geographical location.

Add
Click this button to add an SNMP Manager.

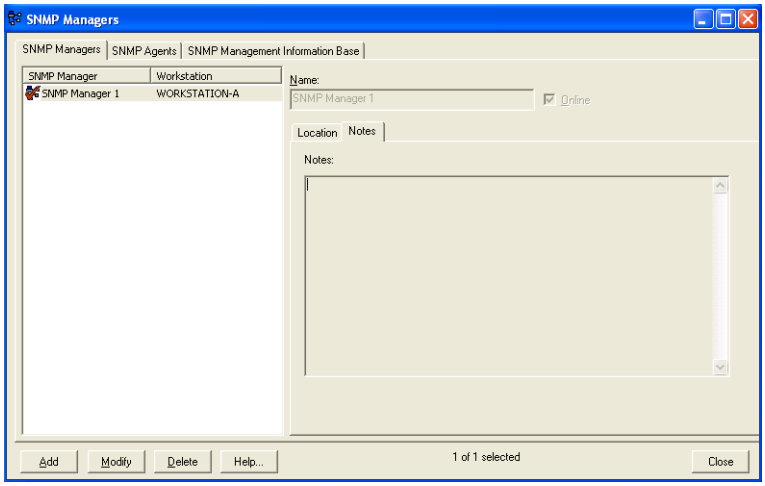
Modify
Click this button to modify an SNMP Manager.

Delete
Click this button to delete an SNMP Manager.

Help
Click this button to display online help for this form.

Close
Click this button to close the SNMP Managers folder.

SNMP Managers Form (Notes Sub-tab)



Notes
Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered shere will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide in Chapter 5, “Monitor Devices.”

SNMP Managers Form Procedures

Use the following procedures on this form.

Add an SNMP Manager

Note: Before SNMP can be configured in OnGuard, the Windows SNMP components must be installed. Instructions for installing the Windows SNMP components, as well as additional information about SNMP can be found in the “Using SNMP with OnGuard” chapter in the Advanced Installation Topics guide.

To add an SNMP Manager:

1. From the ***Additional Hardware*** menu, select ***SNMP Managers***. The SNMP Managers folder opens.
2. On the SNMP Managers tab, click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this SNMP Manager will be assigned to.
   b. Click [OK].
4. In the **Name** field, type a name for the SNMP Manager.
5. Select whether the SNMP Manager will be online.
   a. Allow the **Online** check box to remain selected if you want the SNMP Manager to be ready for use. When an SNMP Manager is online, the Communication Server listens for trap messages from SNMP Agents.
   b. Deselect the **Online** check box if the SNMP Manager is not ready for use. When an SNMP Manager is not online, the Communication Server does not listen for trap messages from SNMP Agents.
6. On the Location sub-tab:
   a. Select the **Workstation** (or server) that the SNMP Manager is or will be running on in order to receive events. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use [Browse] to view a list of available workstations.
   b. Select the world time zone from the **World time zone** drop-down list.
   c. Select whether **Daylight savings** is used or not.

Notes: You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Only one SNMP Manager is allowed to run on each Communication Server. You can have several Communication Servers running with an SNMP Manager on each one and have all Agents in that part of the network configured to report to the local Manager. This would help localize network traffic.

7. Click [OK].

Modify an SNMP Manager

1. From the ***Additional Hardware*** menu, select ***SNMP Managers***.
2. On the SNMP Managers tab, select the entry you want to modify from the listing window.
3. Click [Modify].
4. Make any desired changes.
5. Click [OK].
6. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

Delete an SNMP Manager

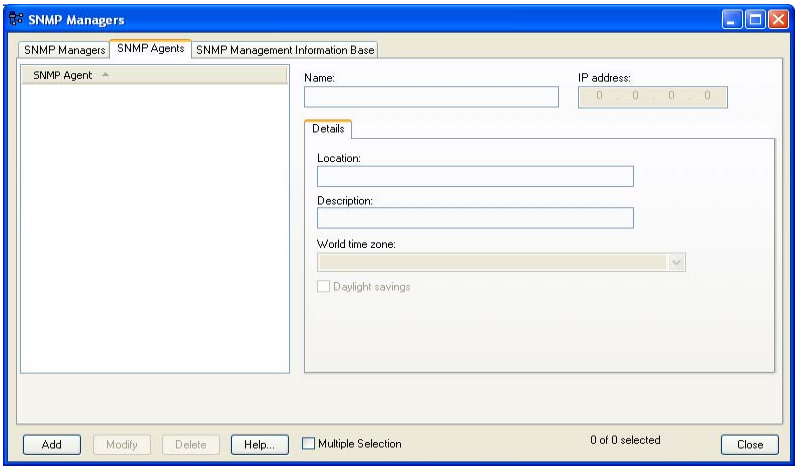
1. From the ***Additional Hardware*** menu, select ***SNMP Managers***.
2. On the SNMP Managers tab, select the entry you want to delete from the listing window.
3. Click [Delete].

4. Click [OK].
5. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

Enter Notes for an SNMP Manager

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].

SNMP Agents Form



Listing window
Lists currently defined SNMP Agents.

Name
Identifies the name of the SNMP Agent. This is a “friendly” name assigned to each SNMP Agent to make it easy to identify.

IP address
Enter the Internet Protocol (TCP/IP) address for the SNMP Agent, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number.

Location
(Optional.) Enter the location of the SNMP Agent.

Description
(Optional.) Enter a description of the SNMP Agent.

World time zone
Select the world time zone for the selected access panel’s geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings
Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Add
Click this button to add an SNMP Agent.

Modify
Click this button to change an SNMP Agent.

Delete
Click this button to delete an SNMP Agent.

Help
Click this button to display online help for this form.

Multiple Selection
If selected, more than one entry in the listing window can be checked simultaneously. The changes made on this form will apply to all selected SNMP Agents.

Close
Click this button to close the SNMP Managers folder.

SNMP Agents Form Procedures

Use the following procedures on this form.

Add an SNMP Agent

If OnGuard receives an event from an Agent that has not been defined, it will automatically add an Agent for it and have the default name set to the IP address of the Agent. You can then go in and modify the **Name** to whatever you want. On a segmented system, Agents are added to the Manager's segment by default, but they can also be assigned to different segments as well.

To add an Agent manually:

1. Select ***SNMP Managers*** from the ***Additional Hardware*** menu. The SNMP Managers folder opens.
2. Click the SNMP Agents tab.
3. Click [Add].
4. In the **Name** field, type a name for the SNMP Agent.
5. In the **IP address** field, enter the IP address of the SNMP Agent.
6. (Optional) In the **Location** field, enter the location of the SNMP Agent.
7. (Optional) In the **Description** field, enter a description of the SNMP Agent.
8. Select the world time zone and daylight savings options as you see fit.

9. Click [OK].

Modify an SNMP Agent

IMPORTANT: If you modify an SNMP Agent, be aware that the cache in Alarm Monitoring will not be updated. If an event for the Agent was already reported and the IP address for the agent is used as its name, that's what will be in the Alarm Monitoring cache and this will not be updated until you log out and then back into Alarm Monitoring.

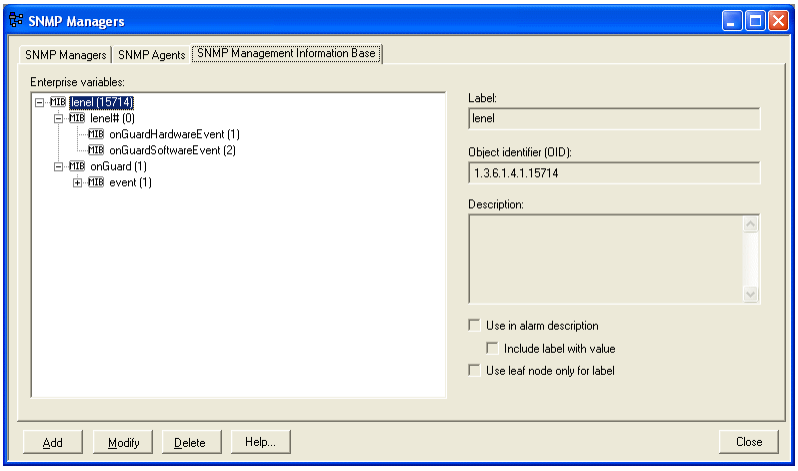
To modify an SNMP Agent:

1. From the ***Additional Hardware*** menu, select ***SNMP Managers***.
2. Click the SNMP Agents tab.
3. Click [Modify].
4. Make any desired changes.
5. Click [OK].
6. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

Delete an SNMP Agent

1. From the ***Additional Hardware*** menu, select ***SNMP Managers***.
2. Click the SNMP Agents tab.
3. Click [Delete].
4. Click [OK].
5. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

SNMP Management Information Base Form



Enterprise variables listing window

Lists all enterprise nodes that are defined in the system and the variables defined for each one (based on what's in the MIB file that was loaded).

Label

The label can be modified.

Object identifier (OID)

All SNMP objects are identified by an Object ID (OID). The string representation of this value is a string of numbers separated by periods. Each number represents a specific object. The base value the OnGuard uses is iso(1).org(3).dod(6).internet(1). This is normally represented 1.3.6.1 and refers to the internet object. Levels below this are expressed using internet as a keyword for 1.3.6.1. Therefore, internet.4.1 is the same as 1.3.6.1.4.1. This identifier refers to the internet.private.enterprises object.

A company's enterprise OID is 1.3.6.1.4.1 followed by their enterprise number (1.3.6.1.4.1.15714 for Lenel). MIB files allow labels to be applied to the numbers in an OID. Using the standard MIB files for SNMP, the enterprise OID would be iso.org.dod.internet.private.enterprises followed by the label for the company's enterprise number provided by their MIB file. In this MIB file, you define all other variables that you will be using. These variables are identified by OIDs. You cannot directly modify an object identifier (OID) - OIDs are determined when a MIB file is loaded.

Description

(Optional) The description can be modified.

Use in alarm description

If selected, the node's information will be used in the alarm description column of Alarm Monitoring if it's present in the trap message. You can have this option set on multiple nodes and for each one that appears in the trap message as a variable, it will be included in the alarm description. When it's included in the alarm description, only the value will be included. The variable name will be discarded.

Include label with value

This check box cannot be selected unless the **Use in alarm description** check box is selected. If this check box is selected, the variable name will appear with the value. When the label is included, the full OID will be displayed. (Actually, it's only the full OID from the enterprise down. The 1.3.6.1.4.1 part gets dropped because that is redundant for all enterprise variables. If it's not an enterprise variable, the entire OID will be displayed.)

Use leaf node only for label

If selected, the SNMP Manager will ignore anything "higher" than the node in the OID.

For example, if a sample variable lenel.onGuard.event.hardwareEvent.description exists and this check box is selected for the lenel.onGuard.event node, then when this variable comes into Alarm Monitoring, only event.hardwareEvent.description will be displayed. This would also apply to all nodes under the event node.

You could go even further and select this check box on the description node so that only "description" is displayed for this node, but for other nodes under event, everything from the event node down is displayed.

Add

Click this button to load a MIB file.

Modify

Click this button to change an enterprise variable. All fields except the Object identifier (OID) can be modified.

Delete
Click this button to delete an enterprise variable.

Help
Click this button to display online help for this form.

Close
Click this button to close the SNMP Managers folder.

SNMP Management Information Base Form Procedures

Use the following procedures on this form.

Load the MIB File(s)

The Management Information Base (MIB) file is used to describe an enterprise's variable structure. The Lenel MIB file is located in the **SNMP** folder on the Supplemental Materials disc. To load an MIB file into OnGuard:

1. Save the MIB file you wish to load to the computer. Remember the location where you save it.
2. If necessary, save any files that contain modules required by the MIB files in the **SNMP-IMPORT-MIBS** folder in the OnGuard installation directory. By default, this is **C:\Program Files\OnGuard\SNMP-IMPORT-MIBS**. The following eight (8) files are installed to that location by default:
   - RFC1155-SMI.txt
   - RFC1213-MIB.txt
   - RFC-1215.txt
   - SNMPv2-CONF.txt
   - SNMPv2-MIB.txt
   - SNMPv2-SMI.txt
   - SNMPv2-TC.txt
   - SNMPv2-TM.txt

Notes: Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

This location can be changed in the **ACS.INI** file by adding the following setting:

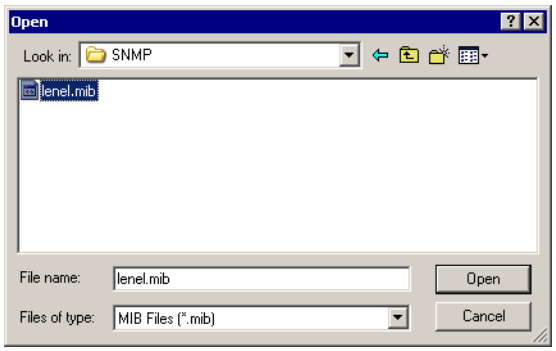
[SNMPManager]

MIBDir="drive:\absolute\path\to\MIB\directory"

This directory is processed when a MIB file is loaded in order to load modules that may be imported into the MIB file being loaded. Only files containing imported modules should be saved in this directory. In most cases, the default files in this directory are sufficient. If additional files are required, determine which additional files define the modules imported by the MIB file and place them in this directory.

If a MIB file for an imported module is not present in this directory and the processor encounters an undefined identifier in the MIB file it's parsing, it will log an error to **MIBProcessor.log** in the OnGuard logs directory.

3. Open System Administration and select ***SNMP Managers*** from the ***Additional Hardware*** menu. The SNMP Managers folder opens.
4. Click the SNMP Management Information Base tab.
5. Click [Add].
6. The Open window is displayed. Navigate to the MIB file you wish to load, and then click [Open]. In this example, the **lenel.mib** file is being loaded.



7. The MIB file will be processed.
   - If the MIB file is successfully parsed, the results will be displayed in the Enterprise variables listing window. You can expand the items in the tree and look at the defined variables.
   - If the MIB file cannot be parsed, an error will be generated, which is written to the **MIBProcessor.log** file. An error is most likely due to a malformed MIB file or a lack of certain MIB files that are imported by the MIB file you are trying to parse.

Note: After a MIB file has been loaded into OnGuard, the actual file is no longer needed.

Modify an SNMP Management Information Base Variable

1. In System Administration, select ***SNMP Managers*** from the ***Additional Hardware*** menu. The SNMP Managers folder opens.
2. Click the SNMP Management Information Base tab.
3. Expand the items in the Enterprise variables listing window.
4. Click on the variable you wish to modify, then click [Modify].
5. Change the **Label** if you wish.
6. Enter a **Description** for the variable if you wish.
7. Select the **Use in alarm description** check box if the node's information will be used in the alarm description column of Alarm Monitoring. You can have this option set on multiple nodes and for each one that appears in the trap message as a variable, it will be included in the alarm description. The variable name will be discarded.
8. Select the **Include label with value** check box if you selected the **Use in alarm description** check box and if you want to see the variable name with the value.
9. Select the **Use leaf node only** check box if you want the SNMP Manager to ignore anything "higher" than this node in the OID.
10. Click [OK].

CHAPTER 59

DataConduIT Sources Folder

DataConduIT is an advanced application integration service that allows real time, bidirectional integration between OnGuard and third party IT sources. DataConduIT allows System Administrators to develop scripts and/or applications that allow events in one domain (security or IT) to cause appropriate actions in the other.

For more information, refer to the DataConduIT User Guide available through

DataConduIT Sources Folder

The DataConduIT Sources folder allows System Administrators to add, modify and delete third-party DataConduIT Sources, Devices, and Sub-Devices. After third-party sources are added, users can send the incoming events to OnGuard via DataConduIT and view third party events in Alarm Monitoring.

To send an event to OnGuard via DataConduIT, System Administrators must:

- Define the incoming source in the DataConduIT Sources folder
- Use the Lnl_IncomingEvent::SendIncomingEvent method

Note: The DataConduIT method has four parameters: the source, description, device (optional), and subdevice (optional). The source of the DataConduIT method must match the source name on the DataConduIT Sources form. If the optional parameters are used, the device of the DataConduIT method must match the device name on the DataConduIT Devices form, and the subdevice must match the sub-device name on the DataConduIT Sub-Devices form.

- Have at least one panel (non-system DataConduIT Source) configured and marked online so that the Communications Server will work properly with DataConduIT Sources. The panel does not need to exist or actually be online in Alarm Monitoring, it simply needs to exist and show up in the System Status view. Once this is set up, events can be successfully received by Alarm Monitoring from DataConduIT Sources.

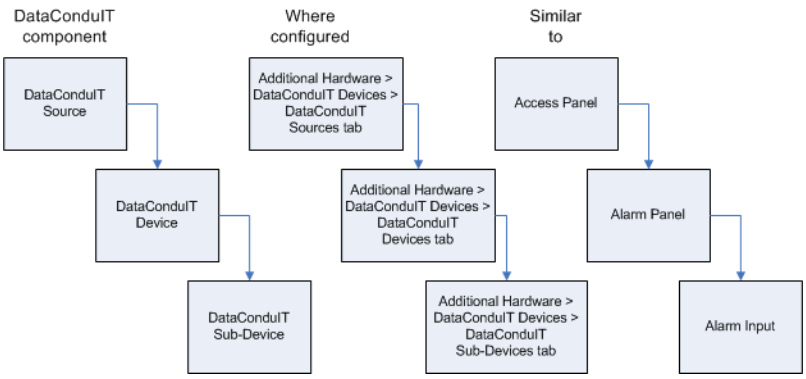
This folder is displayed by selecting ***DataConduIT Sources*** from the ***Additional Hardware*** menu, or by selecting the DataConduIT Sources toolbar button.

Toolbar Shortcut

DataConduIT Source Downstream Devices

A DataConduIT Source may have DataConduIT Device or DataConduIT Sub-Device downstream devices. A DataConduIT Device is a child of a DataConduIT Source, similar to how an alarm panel is a child of an access panel. A DataConduIT Sub-Device is a sub-child device of a DataConduIT Device, similar to how an alarm input is a sub-child of an alarm panel. The diagram that follows illustrates this hierarchy.

DataConduIT Downstream Device Hierarchy



DataConduIT Devices and DataConduIT Sub-Devices also display in Alarm Monitoring in the System Status Tree. For example, a DataConduIT Device named “Tivoli” with a DataConduIT Device named “Tivoli device” and a DataConduIT Sub-Device named “Tivoli sub-device” would display in Alarm Monitoring in the following manner:

Licenses Required

No additional license is required to use the DataConduIT Sources folder other than the “Maximum Number of DataConduIT Clients” license to use DataConduIT in general.

User Permissions Required

DataConduIT Service Permission

The permission required to use DataConduIT in general is the DataConduIT service user permission. This permission is located in Administration > Users > System Permission Groups tab > Software Options sub-tab in System Administration or ID CredentialCenter.

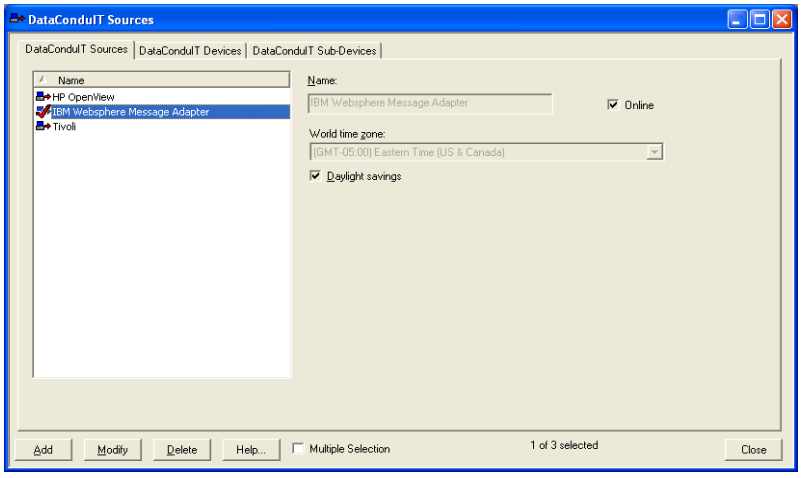
Add, Modify, and Delete DataConduIT Sources, Devices, and Sub-Devices

The add, modify, and/or delete DataConduIT Sources permissions determine what functions a user can perform on DataConduIT Sources, DataConduIT Devices, and DataConduIT Sub-Devices in the DataConduIT Sources folder. These permissions are located in Administration > Users > System Permission Groups tab > Additional Data Sources sub-tab in System Administration or ID CredentialCenter.

Trace DataConduIT Sources, Devices, and Sub-Devices

In addition, user permissions are required to trace DataConduIT Sources, DataConduIT Devices, and DataConduIT Sub-devices in Alarm Monitoring. These permissions are located in Administration > Users > Monitor Permission Groups tab > Monitor sub-tab in System Administration or ID CredentialCenter.

DataConduIT Sources Form



Listing window

Lists DataConduIT Source names.

Name

Identifies the name of the DataConduIT Source. This is a “friendly” name assigned to each DataConduIT Source to make it easy to identify.

Online
If selected, the DataConduIT Source is online and ready for use. To suspend the DataConduIT Source deselect this box.

World time zone
Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings
Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

Add
Click this button to add a DataConduIT Source.

Modify
Click this button to modify a DataConduIT Source.

Delete
Click this button to delete a DataConduIT Source.

Help
Click this button to display online help for this form.

Multiple Selection
If selected, more than one entry in the listing window can be selected simultaneously. The changes made on this form will apply to all selected DataConduIT Sources.

Close
Click this button to close the DataConduIT Sources folder.

DataConduIT Sources Form Procedures

Use the following procedures on this form.

Add a DataConduIT Source

1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***. The DataConduIT Sources folder opens.
2. On the DataConduIT Sources tab, click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this DataConduIT Source will be assigned to.
   b. Click [OK].
4. In the **Name** field, type a name for the DataConduIT Source.

5. Select whether the DataConduIT Source will be online.
6. Select the world time zone and daylight savings options as you see fit.
7. Click [OK].

IMPORTANT: In addition to having a DataConduIT Source configured, there must be at least one panel (non-system DataConduIT Source) configured and marked online so that the Communications Server will work properly with DataConduIT Sources. The panel does not need to exist or actually be online in Alarm Monitoring, it simply needs to exist and show up in the System Status view. Once this is set up, events can be successfully received by Alarm Monitoring from DataConduIT Sources.

Modify a DataConduIT Source

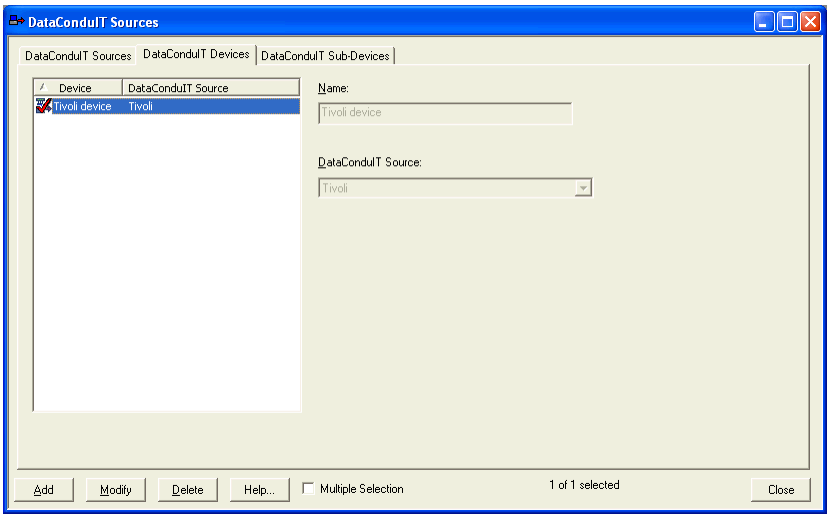
1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***.
2. On the DataConduIT Sources tab, select the entry you want to modify from the listing window.
3. Click [Modify].
4. Make any changes.
5. Click [OK].
6. A prompt to confirm that you want to make the modification displays. Click [OK].

Delete a DataConduIT Source

To suspend a DataConduIT Source without deleting it, take it offline.

1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***.
2. On the DataConduIT Sources tab, select the entry you want to delete from the listing window.
3. Click [Delete].
4. Click [OK].
5. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

DataConduIT Devices Form



Listing window

Lists DataConduIT Device names.

Name

Identifies the name of the DataConduIT Device. This is a “friendly” name assigned to each DataConduIT Device to make it easy to identify.

DataConduIT Source

Select the DataConduIT Source that is the parent of the child device being configured. DataConduIT Sources are configured on the DataConduIT Sources tab (Additional Hardware > DataConduIT Sources > DataConduIT Sources tab).

Add

Click this button to add a DataConduIT Device.

Modify

Click this button to modify a DataConduIT Device.

Delete

Click this button to delete a DataConduIT Device.

Help

Click this button to display online help for this form.

Multiple Selection

If selected, more than one entry in the listing window can be selected simultaneously. The changes made on this form will apply to all selected DataConduIT Devices.

Close

Click this button to close the DataConduIT Sources folder.

DataConduIT Devices Form Procedures

Use the following procedures on this form.

Add a DataConduIT Device

Prerequisite: Before a DataConduIT Device can be configured, its parent DataConduIT Source must first be configured.

Note: If segmentation is enabled, the segment of the DataConduIT Source will be used as the segment for the DataConduIT Device.

1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***. The DataConduIT Sources folder opens.
2. Click the DataConduIT Devices tab.
3. Click [Add].
4. In the **Name** field, type a name for the DataConduIT Device.
5. Select the DataConduIT Source that is the parent of the DataConduIT Device.

Note: The DataConduIT Source must be configured on the DataConduIT Sources tab.

6. Click [OK].

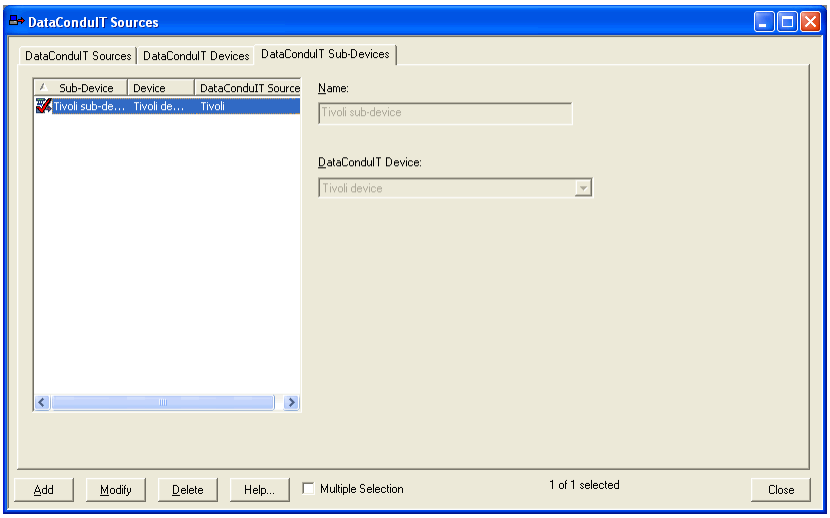
Modify a DataConduIT Device

1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***.
2. Click the DataConduIT Devices tab.
3. Select the entry you want to modify from the listing window.
4. Click [Modify].
5. Make any changes.
6. Click [OK].
7. A prompt to confirm that you want to make the modification displays. Click [OK].

Delete a DataConduIT Device

1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***.
2. Click the DataConduIT Devices tab.
3. Select the entry you want to delete from the listing window.
4. Click [Delete].
5. Click [OK].
6. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

DataConduIT Sub-Devices Form



Listing window

Lists DataConduIT Sub-Device names, along with the parent DataConduIT Device and DataConduIT Source.

Name

Identifies the name of the DataConduIT Sub-Device. This is a “friendly” name assigned to each DataConduIT Sub-Device to make it easy to identify.

DataConduIT Device

Select the DataConduIT Device that is the parent of the child Sub-Device being configured. DataConduIT Devices are configured on the DataConduIT Devices tab (***Additional Hardware*** > ***DataConduIT Sources*** > DataConduIT Devices tab).

Add

Click this button to add a DataConduIT Sub-Device.

Modify

Click this button to modify a DataConduIT Sub-Device.

Delete

Click this button to delete a DataConduIT Sub-Device.

Help

Click this button to display online help for this form.

Multiple Selection

If selected, more than one entry in the listing window can be selected simultaneously. The changes made on this form will apply to all selected DataConduIT Sub-Devices.

Close

Click this button to close the DataConduIT Sources folder.

DataConduIT Sub-Devices Form Procedures

Use the following procedures on this form.

Add a DataConduIT Sub-Device

Prerequisite: Before a DataConduIT Sub-Device can be configured, its parent DataConduIT Source and DataConduIT Device must be configured.

Note: If segmentation is enabled, the segment of the DataConduIT Source will be used as the segment for the DataConduIT Sub-Device.

1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***. The DataConduIT Sources folder opens.
2. Click the DataConduIT Sub-Devices tab.
3. Click [Add].
4. In the **Name** field, type a name for the DataConduIT Sub-Device.
5. Select the DataConduIT Device that is the parent of the DataConduIT Sub-Device.

Note: The DataConduIT Device must be configured on the DataConduIT Devices tab.

6. Click [OK].

Modify a DataConduIT Sub-Device

1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***.
2. Click the DataConduIT Sub-Devices tab.
3. Select the entry you want to modify from the listing window.
4. Click [Modify].
5. Make any changes.
6. Click [OK].
7. A prompt to confirm that you want to make the modification displays. Click [OK].

Delete a DataConduIT Sub-Device

1. From the ***Additional Hardware*** menu, select ***DataConduIT Sources***.
2. Click the DataConduIT Sub-Devices tab.
3. Select the entry you want to delete from the listing window.
4. Click [Delete].
5. Click [OK].
6. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

CHAPTER 60

OPC Connections Folder

The OnGuard OPC Client is a solution for integrating OnGuard with existing third party OPC Servers. The OnGuard OPC Client is an OPC-Alarms and Events client that can connect to any OPC Alarms and Events server. The purpose of the OnGuard OPC Client is to allow OPC Servers to send event and alarm notifications to OnGuard using the OLE for Process Control (OPC) industry standard format.

The OnGuard OPC Client consists of an user interface component to configure OPC Connections and a service component that subscribes to specified OPC Servers to receive event and alarm notifications.

OPC Client Functions

The purpose of the OnGuard OPC Client is to:

- Provide real time communication with any compatible OPC source
- Monitor events and alarms shared by the OnGuard OPC Client and compatible OPC sources

Note: Events and alarms sent by an OPC Server can be viewed, logged and even used to trigger specific actions.

OPC Connections Folder

The OPC Connections folder contains the OPC Connections form and the OPC Sources form from which you can:

- Add, modify or delete OPC Connections
- Test OPC Connections
- Modify the OPC Source name

This folder is displayed by selecting ***OPC Connections*** from the ***Additional Hardware*** menu, or by selecting the OPC Connections toolbar button.

Toolbar Shortcut

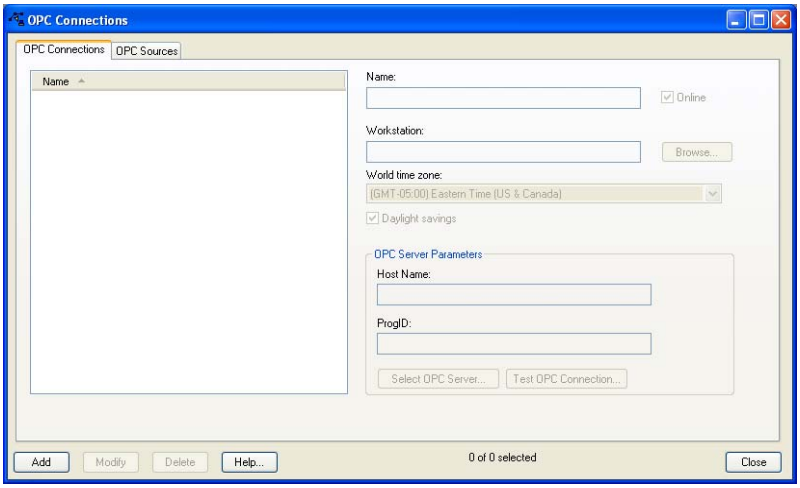
Note: To use this folder an OPC Client support license is required and you must have the correct permissions.

OPC Connections Form

In order to obtain data from an OPC Server, the OnGuard OPC Client must first establish a connection to the OPC Server using standard COM object installation routines. Clients set up two-way communication using connection point interfaces. This communication can be suspended by clients at any time.

The OPC Server can either be local or it can be accessed via DCOM on a remote machine. *DCOM* (Distributed Component Object Model) is a set of Microsoft concepts and program interfaces in which client program objects can request services from server program objects on other computers in a network.

Note: In order to view, add, modify or delete the OPC connection users must have the correct permissions. For more information, refer to System Permission Groups Form Procedures on page 362.



Listing window

Displays the names of OPC connections.

Name

Identifies the name of the OPC connections. This is a “friendly” name assigned to each connection to make it easy to identify. After the OPC Client is added, users can overwrite the default name.

Online

If selected, the OPC connection will be online. To suspend the OPC connection, deselect this box. Select this check box to place the OPC Client online with the OPC Server. This does NOT necessarily mean the OPC Client is online with the actual hardware panel.

Workstation
This is the workstation running the Communication Server. The OnGuard OPC Client is implemented as a device translator. Therefore it is active when the Communication Server is running.

Browse
Browse for the workstation the OnGuard OPC Client is on.

World time zone
Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings
Select this check box if Daylight Savings Time is enforced in the selected access panel's geographical location.

OPC Server Parameters
Includes the Host Name and ProgID fields and the [Select OPC Server] and [Test OPC Connection] push buttons.

Host Name
The computer the OPC Server is on. To populate the Host Name and ProgID fields, click the [Select OPC Server] button.

ProgID
The OPC Server's global unique identifier. To populate the Host Name and ProgID fields, click the [Select OPC Server] button.

Select OPC Server
Displays the Select OPC Server window which enables you to select the OPC Server by searching for it or manually entering it.

Test OPC Connection
Tests a specified OPC Connection. When the OPC connection is successful the OPC Server Properties window displays the current OPC Server status.

The client to server connection is tested. The client to alarm panel connection is NOT tested.

Add
Adds an OPC connection.

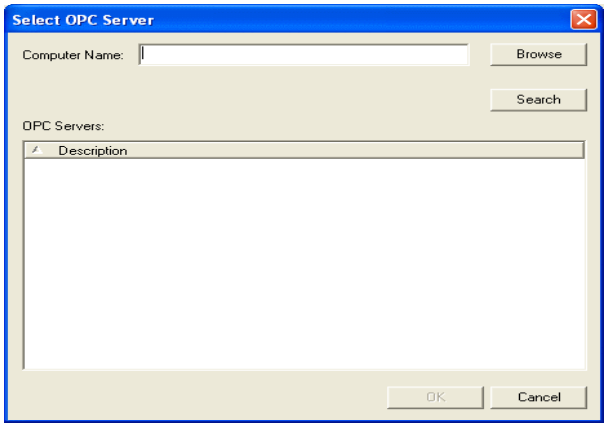
Modify
Modifies or suspends an OPC connection.

Delete
Deletes an OPC connection.

Help
Displays online help for this form.

Close
Closes the OPC Connections folder.

Select OPC Server Window



Computer Name
Enter the name of the computer the OPC Server is on.

Browse
Browse all available computers on the network.

Search
Searches the specified computer for OPC Servers that are on it.

OPC Servers Listing Window
Displays the OPC Servers on the specified computer.

OK
Adds the OPC Server parameters to the OPC Connections form.

Cancel
Cancels the current selection and closes the Select OPC Server window.

OPC Connections Form Procedures

Use the following procedures on this form.

Add an OPC Connection

1. From the ***Additional Hardware*** menu, select ***OPC Connections***. The OPC Connections folder opens.
2. On the OPC Connections tab, click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:

a. The Segment Membership window opens. Select the segment that this OPC connection will be assigned to.
b. Click [OK].

4. In the **Name** field, type a name for the OPC connection.
5. Select whether the OPC connection will be online.

   IMPORTANT: When the OPC connection shows up as online, that means it is online with the OPC Server and NOT necessarily online with the actual hardware panel.

6. Select or enter the workstation the Communication Server is running on.
7. Click [Select OPC Server]. The Select OPC Server window displays.
   a. Enter or browse the name of the computer the OPC Server is on.
   b. Click [Search]. The OPC Servers on the specified computer display.
   c. Select (place a checkmark beside) the correct OPC Server and click [OK].
8. Select the world time zone and daylight savings options as you see fit.
9. The Host Name and Program ID fields automatically populate on the OPC Connections form.
10. Click [Test OPC Connection] to verify the OPC connection is successful and to view the current OPC Server status.
11. Click [OK].

Modify an OPC Connection

1. From the ***Additional Hardware*** menu, select ***OPC Connections***.
2. On the OPC Connections tab, select the entry you want to modify from the listing window.
3. Click [Modify] and make the appropriate modifications. To suspend an OPC Connection take it offline.
4. Click [OK].
5. A prompt to confirm that you want to make the modification will be displayed. Click [OK].

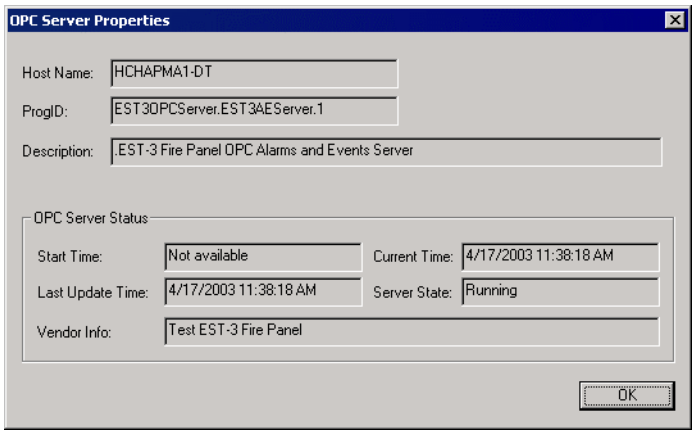
Delete an OPC Connection

To suspend an OPC Connection without deleting it, take it offline.

1. From the ***Additional Hardware*** menu, select ***OPC Connections***.
2. On the OPC Connections tab, select the entry you want to delete from the listing window.
3. Click [Delete].
4. Click [OK].
5. A prompt to confirm that you want to make the deletion will be displayed. Click [OK].

Test OPC Connection

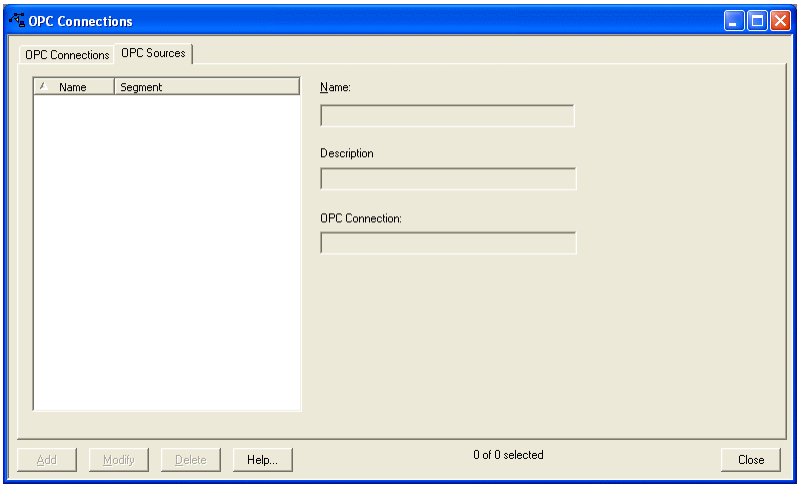
1. From the ***Additional Hardware*** menu, select ***OPC Connections***.
2. Open the OPC Connections tab and select the OPC Client.
3. Click [Modify].
4. Click [Test OPC Connection].
5. If the test is successful the OPC Server Properties window displays and contains real time data about the OPC Server.



OPC Sources Form

While the OnGuard OPC Client is connected to a particular OPC Server, it can receive event notifications from that server and send event information to monitoring stations. When the OnGuard OPC Client receives an event from the OPC Server the source is automatically added to the OPC Sources form listing window.

System Administrators cannot manually add OPC Sources to the OPC Sources form listing window. The [Add] button will always be grayed out. System Administrators can however, modify the OPC Source name. This is also the name that displays in Alarm Monitoring under the Device column of the alarm view as well as in the system status tree.



Listing window

Lists the active OPC connections.

Name

The name for the selected OPC source. Users can modify this name which also displays in Alarm Monitoring.

Description

The original name of the OPC source. The description is read only.

OPC Connection
Identifies the OPC Server the client is connected to. This is a read only field.

Add
Does not apply. For more information, refer to OPC Connections Folder on page 1177.

Modify
Click this button to modify the OPC source name

Delete
Click this button to delete the OPC source.

Help
Click this button to display online help for this form.

Close
Click this button to close the OPC Connections folder.

OPC Sources Form Procedures

Use the following procedures on this form.

Modify OPC Source Name

1. From the ***Additional Hardware*** menu, select ***OPC Connections***.
2. Open the OPC Sources tab.
3. Select an OPC Source.
4. Click [Modify].
5. Edit the OPC Source Name.
6. Click [OK].

Delete OPC Source

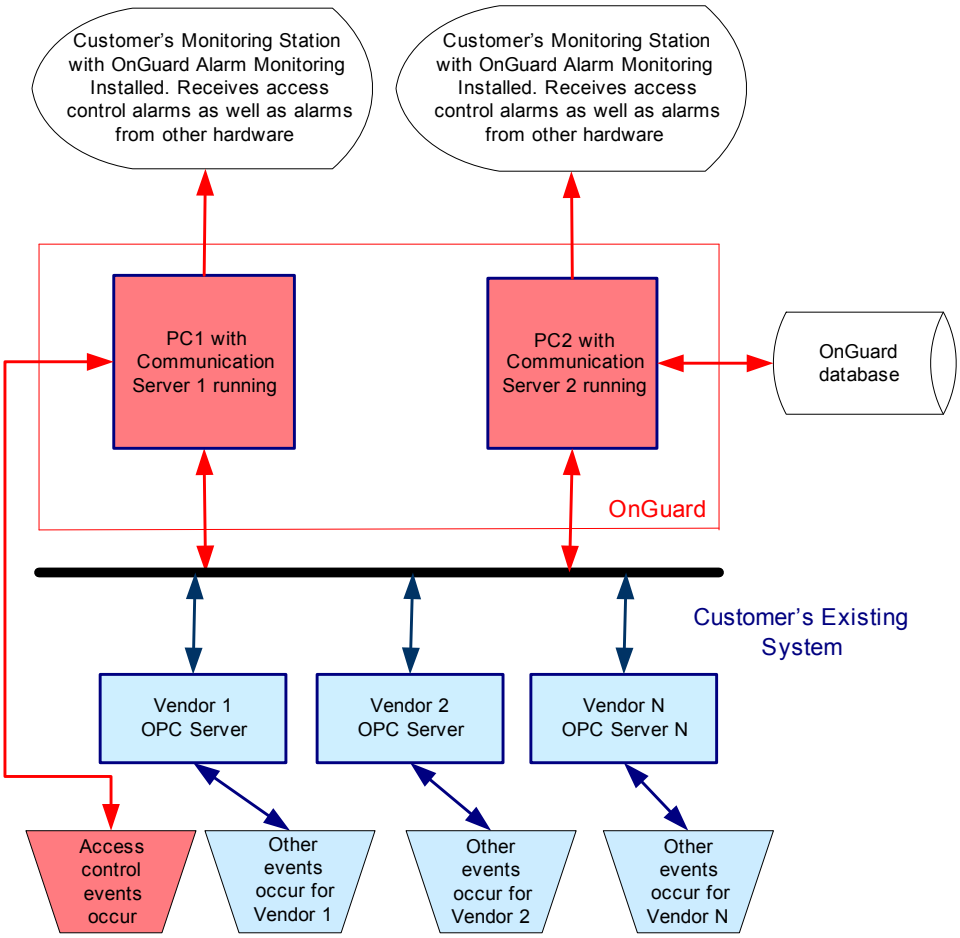
1. From the ***Additional Hardware*** menu, select ***OPC Connections***.
2. Click the OPC Sources form/tab.
3. Select an OPC Source.
4. Click [Delete] to temporarily discontinue the OPC connection.

OnGuard OPC Client Scenario

Let’s look at a hypothetical customer in the airline industry. This customer has an existing central control room with several OPC compliant servers monitoring every flight and traveler information.

New high security access control card readers, cameras and motion detectors have been installed and the customer wants to integrate this with their existing systems and monitor access control alarms and events from the same control room.

How does the customer monitor the access control alarms and events using the existing OPC Servers?



By making OnGuard an OPC Client, the customer can use OnGuard to communicate directly with their existing OPC Servers. To make OnGuard an OPC Client the OPC support license must be purchased.

The OnGuard OPC Client, receives and translates alarms and events from the OPC Server and outputs them in the Alarm Monitoring application along with the alarm and events received from the newly installed access control system.

Displaying Data

The OnGuard OPC Client supports every event attribute required by OPC specifications. The following table indefinites how OPC event attributes are mapped to OnGuard events. Note that the source name attribute can be modified to a user-friendly name.

OPC event attribute	Description	OnGuard event attribute in Alarm Monitoring alarm view
OPC Connection Description	Identifies the OPC Server that the OnGuard OPC Client is communication with.Text description of the OPC connection configured in System Administration. This is also the name of the controller when configuring monitor zones.	“Controller” field in alarm view
Source	The object which generated the event.	“Device” field in alarm view
Message	Text which describes the event.	“Event description” field in alarm view
Event Category	The vendor-specific category which this event belongs.	Part of the “Associated Text” field in alarm view
Severity	The urgency of the event.	Alarm priority
Condition Name	The name of the OPC condition/alarm related to the event notification.	Part of the “Associated Text” field in alarm view
Quality	The current quality of the data.	Part of the “Associated Text” field in alarm view

Logical Access

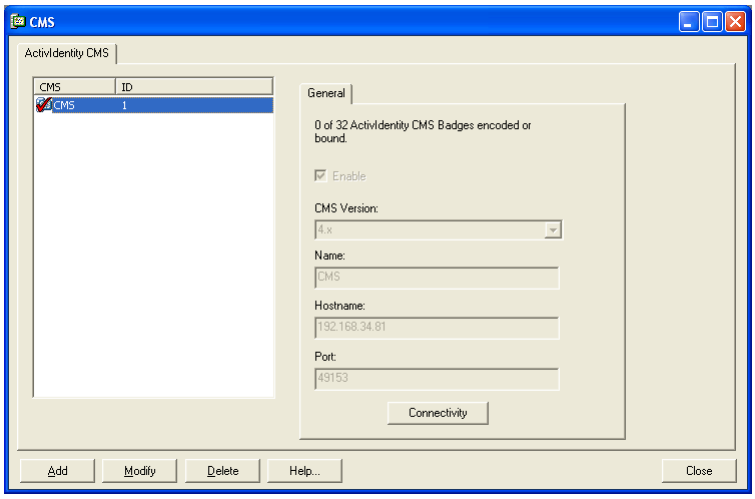
CHAPTER 61

CMS Folder

The CMS folder contains one form, which is the ActivIdentity CMS form. For detailed information about the CMS feature, refer to Appendix I: Integrating ActivIdentity CMS with OnGuard on page 1453..

This folder is displayed by selecting ***ActivIdentity*** from the ***Logical Access*** menu in System Administration or ID CredentialCenter.

ActivIdentity CMS Form



Listing window

Lists the name and ID of currently defined ActivIdentity CMS systems.

Enable

If the CMS server is online and you wish to connect to it, leave the **Enable** check box selected. If not, deselect the **Enable** check box. The **Enable** check box must be selected in order to enter the name, hostname, and port for the CMS server.

CMS Version
Select the major version of the CMS server.

Name
A unique name that you specify to identify the CMS with. This name does not have to correlate to any name used in CMS.

Hostname
Name of the machine hosting CMS.

Port
Port on which CMS is listening for requests.

Connectivity
Before clicking [Connectivity], you must either add a new CMS and fill in the **CMS Version**, **Name**, **Hostname**, and **Port** fields, or select an existing CMS record in the listing window. When you click [Connectivity], the OnGuard system will attempt to connect to the desired CMS.

SSL protocol with mutual authentication is used during interactions between OnGuard and CMS. In order to connect to CMS, an operator must have valid credentials (a certificate). This certificate must be enrolled in CMS as the operator's certificate. Upon receiving requests for operations from OnGuard, CMS verifies that the role assigned to the operator's credential is allowed to perform this operation.

Add
Click this button to add a CMS.

Modify
Click this button to change a CMS.

Delete
Click this button to delete a CMS.

Help
Displays online help for this form.

Close
Closes the CMS folder.

CMS Folder Procedures

For instructions on how to configure and use CMS, refer to Appendix I: Integrating ActivIdentity CMS with OnGuard on page 1453.. The following procedures in that section are performed in this folder:

- Add a CMS Connection on page 1457
- Verify Connectivity to the Selected CMS on page 1458

Appendices

APPENDIX A

Actions

Actions can be added (configured) through the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O folders in System Administration. Actions can also be added through the Scheduler in Alarm Monitoring.

If you add an action through the Scheduler or Guard Tour folder, you can also schedule the action to execute routinely or once. To manually execute an action you can right-click a device in Alarm Monitoring > System Status window.

This appendix describes how to add (configure) an action to your OnGuard system.

IMPORTANT: For the Scheduler to be able to execute actions the Linkage Server must be configured and running. You can configure the Linkage Server host on the General System Options form in the System Options folder. For more information, refer to General System Options Form on page 392.

NGP Actions

The following actions are available for the NGP access panel:

- Arm/Disarm Area
- Deactivate Badge
- Device Output
- Device Output Group
- Global APB System / Segment Reset
- Grant Deny Popup
- ISC Firmware Download
- ISC Database Download
- Mask/Unmask Alarm Input
- Mask/Unmask Alarm Input for Input Group
- Mask/Unmask Door
- Mask/Unmask Door Forced Open

- Mask/Unmask Door Forced Open for Reader Group
- Mask/Unmask Door Held Open
- Mask/Unmask Door Held Open for Reader Group
- Move Badges for APB Area
- Muster Mode Initiation
- Pulse Open Door
- Pulse Open Door Group
- Reader Mode
- Reader Mode Group
- Sign Out Visitor
- Silence Area

General Actions Procedures

The following procedures can be performed on this form.

Specify the Number of Simultaneous Actions

IMPORTANT: Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

Occasional problems may occur when running a large number of actions at once. OnGuard defaults the limit of simultaneous actions to fifty but that can be changed in the **ACS.INI** file.

To change the ACS.INI file to override the default limit on simultaneous actions:

1. In the Windows start menu click run.
2. In the Run dialog box type “ACS.INI” without the quotes.
3. In the ACS.INI file find the [Service] section and add the line: “MaxNumberActionThreads=<Number of actions>” without the quotes and where the “Number of actions” equals the number of simultaneous actions you want to occur.

Open an Action Properties Window

Refer to the following procedures to open an action properties window through various folders in System Administration and Alarm Monitoring.

Using Action Group Library

The Action Group Library folder can be used to group actions. For more information, refer to Chapter 25: Action Group Library Folder on page 525.

Note: To schedule a group of actions or configure a group of actions based on incoming events, guard tour related conditions, or acknowledged alarms, you can use the action type called “Action group” which is available using the Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O folders. For more information, refer to Add an Action Group on page 1197.

1. In System Administration, select ***Action Group Library*** from the ***Administration*** menu.

2. Click [Add].
3. The Action Group Properties window displays.
4. Enter an action group name and click [Add].
5. The Select Action Type window opens. Select the appropriate action and click [Next]. The Action Properties window opens.

Using the Scheduler

The Scheduler folder can be used to configure actions to occur on a schedule (reoccurring or one time only). For more information, refer to Chapter 24: Scheduler Folder on page 515.

Toolbar Shortcut

1. In System Administration, select ***Scheduler*** from the ***Administration*** menu. In Alarm Monitoring, click the Scheduler toolbar button.
2. Click [Add]. The Add Action Wizard window displays.
3. In the Category listing window, select “Action Types” and in the Objects listing window, select the appropriate action.
4. Click [Next]. The Action Properties window opens.

Using Global I/O

The Global I/O folder can be used to configure actions to occur based on an incoming event. For more information, refer to Chapter 38: Global I/O Folder on page 805.

1. In System Administration, select ***Global I/O*** from the ***Access Control*** menu.
2. Select a global linkage.
3. Click [Modify].
4. On the Output Action tab, click [Add].
5. The Add Action Wizard window displays. In the Category listing window, select “Action Types” and in the Objects listing window, select the appropriate action.
6. Click [Next]. The Action Properties window opens.

Using Guard Tour

The Guard Tour folder can be used to configure actions to occur under certain conditions related to a guard tour. For more information, refer to Chapter 45: Guard Tour Folder on page 891.

1. In System Administration, select ***Guard Tour*** from the ***Monitoring*** menu. You cannot configure an action using the Guard Tour option available in Alarm Monitoring.
2. On the Tours tab, highlight a tour.
3. Click [Modify].
4. The Tour Wizard window opens. Select (place a checkmark beside) an ID/hardware device.
5. Click [Next].
6. Click [Add].
7. The Add Action Wizard window displays. In the Category listing window, select “Action Types” and in the Objects listing window, select the appropriate action.
8. Click [Next]. The Action Properties window opens.

Using Acknowledgment Actions

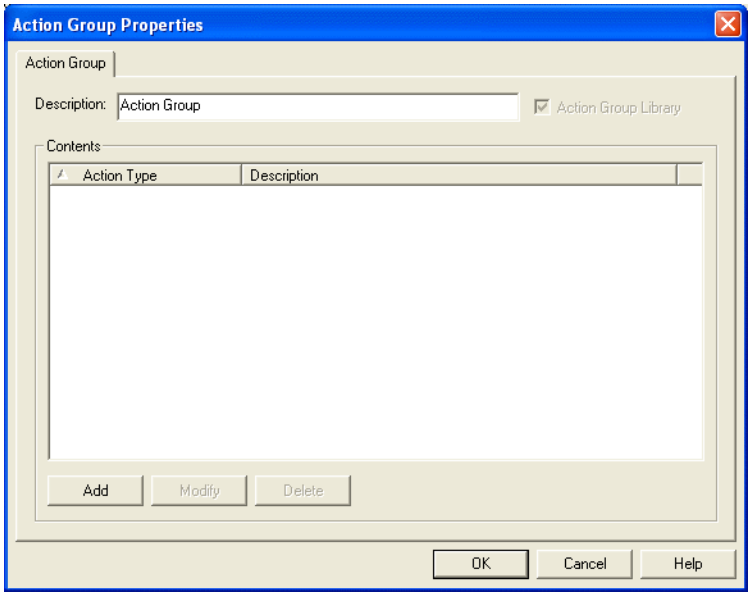
The Acknowledgment Actions folder can be used to configure actions to occur when an alarm is acknowledged. For more information, refer to Chapter 43: Alarm Configuration Folder on page 849.

1. In System Administration, select ***Alarms*** from the ***Monitoring*** menu.
2. Click the Acknowledgment Actions tab.
3. Select (place a checkmark beside) an alarm.
4. Click [Modify].
5. In the Actions section, click [Add].
6. The Add Action Wizard window displays. In the Category listing window, select “Action Types” and in the Objects listing window, select the appropriate action.
7. Click [Next]. The Action Properties window opens.

Action Group Properties Window

The Action Group Properties action executes multiple actions simultaneously.

You can display the Action Group Properties window using the Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O forms. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Description

When adding or modifying an action group, you can enter a description of the action group that is being configured.

Action Group Library

When selected, the action group that you are adding or modifying will be available for selection in the Action Group Library. For more information, refer to Chapter 25: Action Group Library Folder on page 525.

Action Type listing window

Displays the action types which have been assigned to the selected action group.

Add

Click this button to add an action type.

Modify

Click this button to modify the action type that is selected in the Action Type listing window.

Delete

Click this button to delete the action type that is selected in the Action Type listing window from the selected action group.

OK

Click this button to save your changes and exit out of the Action Group Properties window.

Cancel

Click this button to exit the Action Group Properties window without saving your changes.

Help

Click this button to display online help for this window.

Action Group Properties Window Procedures

The following procedures can be performed on this form.

Add an Action Group

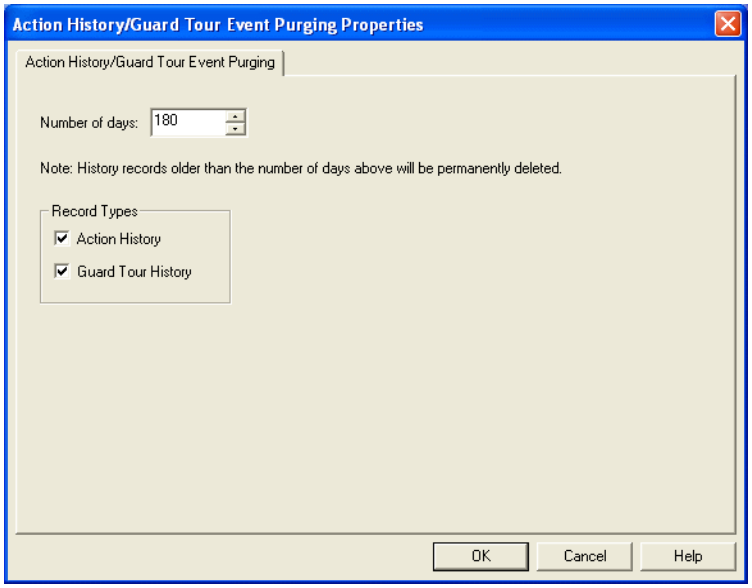
1. Open the Action Group Properties window using the Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. In the **Description** field, enter a description of the action group that is being configured.
3. Select the **Action Group Library** check box if you want this action group to be available for selection in the Action Group Library. For more information, refer to Action Groups Overview on page 525.
4. Click [Add]. The Select Action Type window opens.
5. Select an action type and then click [Next]. Depending on which action type you chose, a corresponding action properties window will open.
6. Configure the action type you selected in step 5. To do this, you must refer to the action properties windows sections in this chapter for information on each action properties window.
7. Repeat steps 4-6 for each action type you want to assign to this group.
8. Click [OK].

Action History/Guard Tour Event Purging Properties Window

The Action History/Guard Tour Event Purging action allows you to create an action that will automatically delete certain records after they are a specified number of days old. For example, you can have all Guard Tour History record types deleted when they are 180 days old.

You can display the Action History/Guard Tour Event Purging Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.

Note: In segmented systems, the Action History/Guard Tour Event Purging action must be applied to all segments.



Number of Days

The history records older than the number of days selected will be permanently deleted when the action runs.

Action History

Select this check box if you want Action History records deleted that are older than the Number of days setting.

Guard Tour History

Select this check box if you want Guard Tour History records deleted that are older than the Number of days setting.

OK

Click this button to add the action and exit out of the Action History/Guard Tour Event Purging Properties window.

Cancel

Click this button to exit the Action History/Guard Tour Event Purging Properties window without adding the action.

Help

Click this button to display online help for this window.

Action History/Guard Tour Event Purging Properties Window Procedures

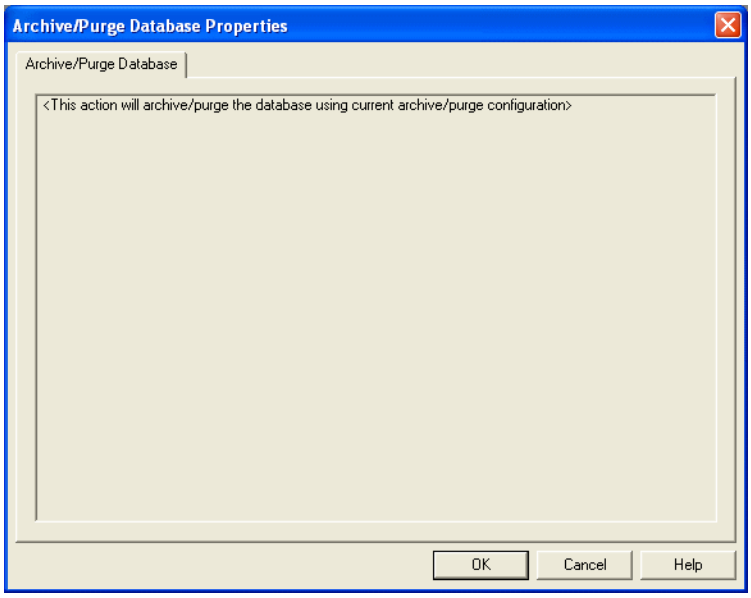
The following procedures can be performed on this form.

Add an Action History/Guard Tour Event Purging Action

1. Open the Action History/Guard Tour Event Purging Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Enter how old (number of days) records can be before they are purged.
3. Choose the type of records you want to delete.
4. Click [OK]. This action is now configured to archive/purge the database using your current archive/purge configurations.

Archive/Purge Database Properties Window

You can display the Archive/Purge Database Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.



Notes: In segmented systems, the Archive/Purge Database Properties action must be applied to all segments.

If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Listing window

Displays the following message: "<This action will archive/purge the database using current archive/purge configuration>"

OK

Click this button to add the action and exit out of the Archive/Purge Database Properties window.

Cancel

Click this button to exit the Archive/Purge Database Properties window without adding the action.

Help

Click this button to display online help for this window.

Archive/Purge Database Properties Window Procedures

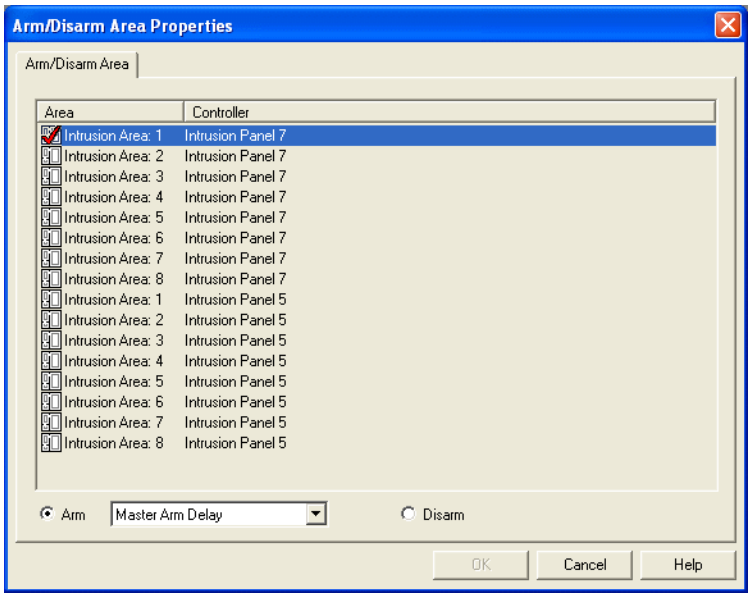
The following procedures can be performed on this form.

Add an Archive/Purge Database Action

1. Open the Archive/Purge Database Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Click [OK]. This action is now configured to archive/purge the database using your current archive/purge configurations. For more information, refer to Chapter 23: Archives Folder on page 501.

Arm/Disarm Area Properties Window

You can display the Arm/Disarm Area Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Listing window

Lists currently enabled intrusion areas. Intrusion areas are configured on the Areas form in the Intrusion Detection Configuration folder. For more information, refer to Areas Form on page 1140.

Arm

When configuring an area as an action, select this radio button if you want the action to be that the area will be armed. When an area is armed, protection for this area is "turned on." Alarms will be reported within the area (the zones within the area will report alarms when activated).

For example, consider a home burglar system that has sensors on the windows and doors and motion detectors inside. When the owner leaves the home, they arm the system. Alarms will be reported if those windows/doors are opened or if motion is detected.

You must also select an option from the drop-down list. The following terms will help you choose an option.

Instant arm - some intrusion panels support the notion of both delay arm and instant arm. With instant arm, the area is armed immediately.

Interior and Perimeter- in higher end intrusion panels, there is the concept of an interior and a perimeter of an area. Various zones within the area are associated with either the interior or the perimeter. Zones that might be associated with the interior are motion detectors placed in the hallways of an office building. Zones that might be associated with the perimeter are sensors on external windows and doors.

Master arm - when an area is master armed, the entire area is armed. This includes both the perimeter and the interior.

Perimeter arm - when an area is perimeter armed, only the perimeter is armed. This means that those zones associated with the interior will continue to generate alarms, but those associated with the perimeter will not. This type of arming may be used when an authorized person is inside a building at off hours. They don't want the interior armed and reporting alarms since they will be moving throughout the interior. However, if somebody else breaches the perimeter of the building (forces open a door, breaks a window, etc.), alarms will be reported. (continued on next page)

Partial arm - arms only those zones that have been configured for partial arming. All other zones in the area will not be armed.

For Detection Systems intrusion detection panel types, choices include:

- Arm Entire Partition - arms both the interior and perimeter of the area.
- Perimeter Arm - arms the perimeter of the area.

For Bosch intrusion detection panel types, choices include:

- Master Arm Delay - master (both perimeter and interior) arm (with exit and entry delays) the area.
- Master Arm Instant - master (both perimeter and interior) arms (no delays) the area.
- Perimeter Delay Arm - delay arms all perimeter points in the area.
- Perimeter Instant Arm - instantly arms all perimeter points (no delays) in the area.

For Galaxy intrusion detection panel types, choices include:

- Arm Entire Partition - arms both the interior and perimeter of the area.
- Partial Arm - arms only those zones that have been configured for partial arming. All other zones in the area will not be armed.

Disarm

When configuring an area as an action, select this radio button if you want the action to be that the area will be disarmed. When an area is disarmed, protection for this area is "turned off." Alarms will not be reported within the area.

For example, consider a home burglar system that has sensors on the windows and doors and motion detectors inside. When the owner arrives home, he/she disarms the system so that alarms won't be reported as they walk around the house.

OK

Click this button to add the action and exit out of the Arm/Disarm Area Properties window.

Cancel

Click this button to exit the Arm/Disarm Area Properties window without adding the action.

Help

Click this button to display online help for this window.

Arm/Disarm Area Properties Window Procedures

The following procedures can be performed on this form.

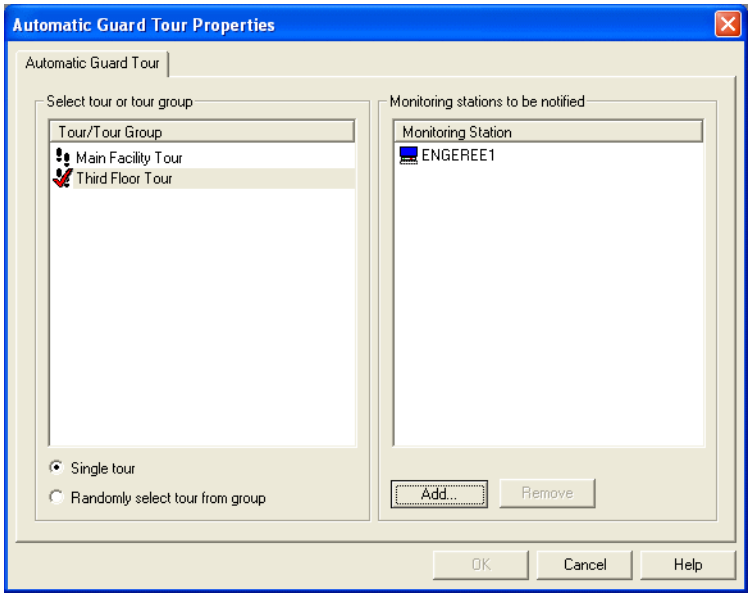
Add an Arm/Disarm Area Action

1. Open the Arm/Disarm Area Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. From the listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Arm** radio button if you want the action to be that the area will be armed. You must also select an option from the drop-down list.
   - Select the **Disarm** radio button if you want the action to be that the area will be disarmed.

   IMPORTANT: Refer to Arm/Disarm Area Properties Window Procedures on page 1202 for detailed information on arming and disarming areas.
4. Click [OK].

Automatic Guard Tour Properties Window

You can display the Automatic Guard Tour Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed the Automatic Guard Tour Properties window via the Scheduler form, the window will contain both the Automatic Guard Tour form and the Scheduler form.

Tour/Tour Group listing window

Displays a list of the tours and tour groups which have been configured in the system. Tours and tour groups are configured in the Guard Tour folder.

Single tour

Select this radio button if you want to configure an automatic guard tour for a single tour. When selected, only single tours will be listed in the Tour/Tour Group listing window.

Randomly select tour from group

Select this radio button if you want to configure an automatic guard tour that will be randomly selected from a tour group. When selected, only tours groups that are configured as random tour lists will be listed in the Tour/Tour Group listing window. Tour groups are configured on the Tour Groups form of the Guard Tour folder. A tour group is considered a random tour list when the **Random Tour List** check box is selected on the Tour Groups form.

Monitoring Station listing window

Displays a list of the monitoring stations which are assigned to the selected tour. These monitoring stations will be notified when the automatic guard tour is scheduled to begin.

Add

Click this button to display the Select Monitoring Station window and add a monitoring station to the Monitoring Station listing window.

Remove

Click this button to remove the selected monitoring station from the Monitoring Station listing window.

OK

Click this button to add the action and exit out of the Automatic Guard Tour Properties window.

Cancel
Click this button to exit the Automatic Guard Tour Properties window without adding the action.

Help
Click this button to display online help for this window.

Automatic Guard Tour Properties Window Procedures

The following procedures can be performed on this form.

Add an Automatic Guard Tour Action

1. Open the Automatic Guard Tour Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Do one of the following:
   - Select the **Single Tour** radio button if you want to configure an automatic guard tour for a single tour. When selected, only single tours will be listed in the Tour/Tour Group listing window.
   - Select the **Randomly select tour from group** radio button if you want to configure an automatic guard tour that will be randomly selected from a tour group. When selected, only tours groups that are configured as random tour lists will be listed in the Tour/Tour Group listing window.
3. The monitoring stations that have been assigned to the selected tour or tour group will be displayed in the Monitoring Station listing window. Do one of the following:
   - If no monitoring stations have been assigned or if you want to assign an additional monitoring station, then click [Add]. The Select Monitoring Station window opens.
   - If you do not want to assign a monitoring station, proceed to step 7.
4. Click on a monitoring station to select it.
5. Click [OK]. The monitoring station you selected will be listing in the Monitoring Station listing window. All monitoring stations in the Monitoring Station listing window will, in the Alarm Monitoring application, receive a notification message when the tour is scheduled to begin.
6. Repeat steps 3-5 for each monitoring station you want to add.

Note: If you want to remove a monitoring station from the Monitoring Station listing window, click on an entry to select it and then click [Remove].

7. Click [OK].

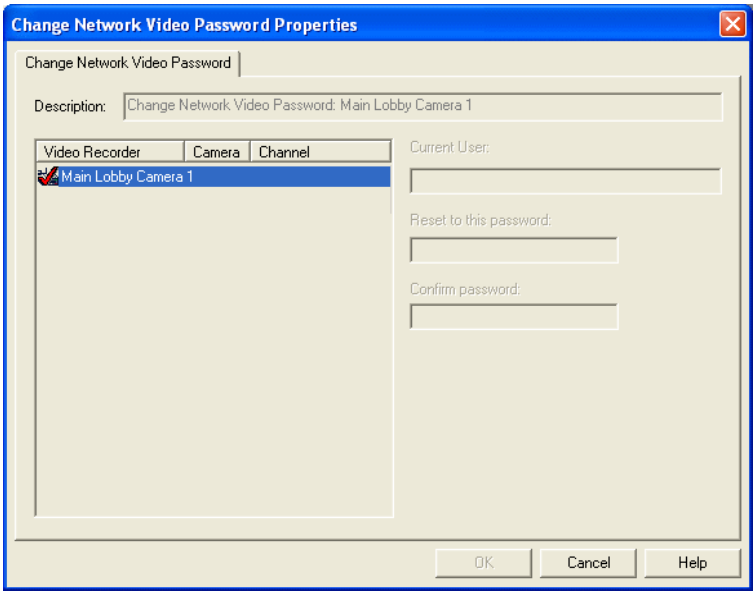
Note: If you have accessed the Automatic Guard Tour Properties window via the Scheduler folder or the Scheduler form in the Guard Tour folder, the window will contain both the Automatic Guard Tour form and the Schedule form. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Change Network Video Password Properties Window

The Change Network Video Password action allows you to schedule automatic password changes for video recorders. You can make the change a one-time event or to schedule it daily, weekly, or monthly

with the Edit Recurring Action Schedule. For more information, refer to Chapter 24: Scheduler Folder on page 515.

You can display the Change Network Video Password Properties window using the Action Group Library, Scheduler, or Global I/O. Only the Scheduler will let you set up the password to be changed at a later date. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Description

Names the video device you are currently changing the password for.

Listing Window

Lists currently defined LNVR recorders and cameras associated with them.

Select the recorders and/or cameras you want to modify.

Current User

The name of the user account.

This field automatically populates if a user name was initially populated on the Video Recorder/ Camera forms.

Reset to this password

Enter the password in the text box. The following restrictions apply:

- Axis cameras allow up to 10 character passwords using A through Z, a through z, 0 - 9, !, #' - ', -, ., ^, _, ~, $
- Sony cameras allow up to 16 character passwords using A through Z, a through z, 0 - 9
- LNVR recorder password length is limited by the LNVR's computer password policy, which is set by the system administrator. Valid characters are ! - ~

Note: In addition to these restrictions, OnGuard includes strong password enforcement, which checks the user's password against password standards. For more information, refer to Introduction to System Administration on page 49.

Confirm password
Enter the password a second time for verification.

OK
Adds the action and exits out of the Change Network Video Properties window.

Cancel
Exits the Change Network Video Password Properties window without adding the action.

Help
Displays online help for this window.

Change Network Video Password Properties Window Procedures

The following procedures can be performed on this form.

Change the Network Video Password

1. Open the Change Network Video Password Properties window using the Action Group Library or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. On the Change Network Video Password tab, enter the new password and confirm the password by typing it again.
3. Click [OK].

Schedule a One-Time Password Change

1. Open the Change Network Video Password Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. On the Change Network Video Password tab, enter the new password and confirm the password by typing it again.
3. On the Schedule tab, select the **One time** radio button.
4. Select the date and time you wish the password to change.
5. Click [OK].

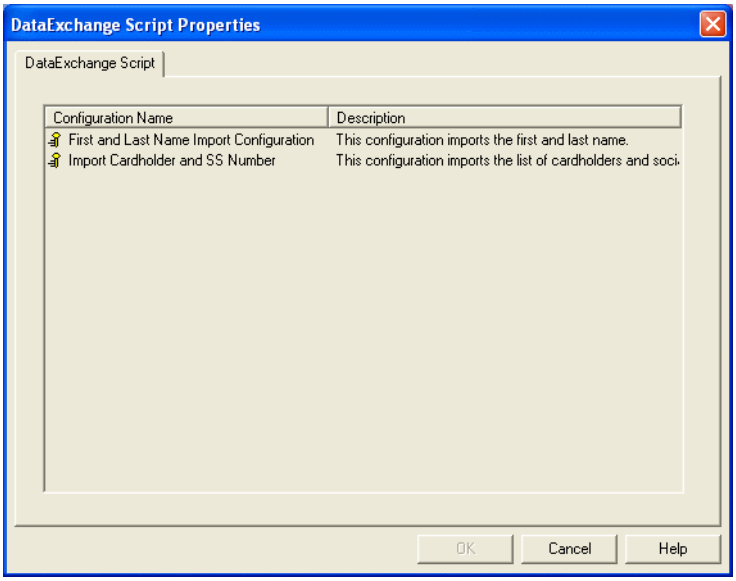
Schedule a Recurring Password Change

1. Open the Change Network Video Password Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. On the Change Network Video Password tab, enter the new password and confirm the password by typing it again
3. On the Schedule sub-tab, select the **Recurring** radio button.
4. Click [Change]. The Edit Recurring Action Schedule form displays.
5. Choose the time and date intervals that best suit your needs.
6. Click [OK] on the Edit Recurring Action Schedule form.

7. Click [OK] on the Change Network Video Password Properties window.

DataExchange Script Properties Window

You can display the DataExchange Script Properties window using Scheduler. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Configuration Name listing window

Displays a list of the DataExchange configurations that have been configured in the system. DataExchange configurations are created in FormsDesigner.

OK

Click this button to add the action and exit out of the DataExchange Script Properties window.

Cancel

Click this button to exit the DataExchange Script Properties window without adding the action.

Help

Click this button to display online help for this window.

DataExchange Script Properties Window Procedures

The following procedures can be performed on this form.

Add a DataExchange Script Action

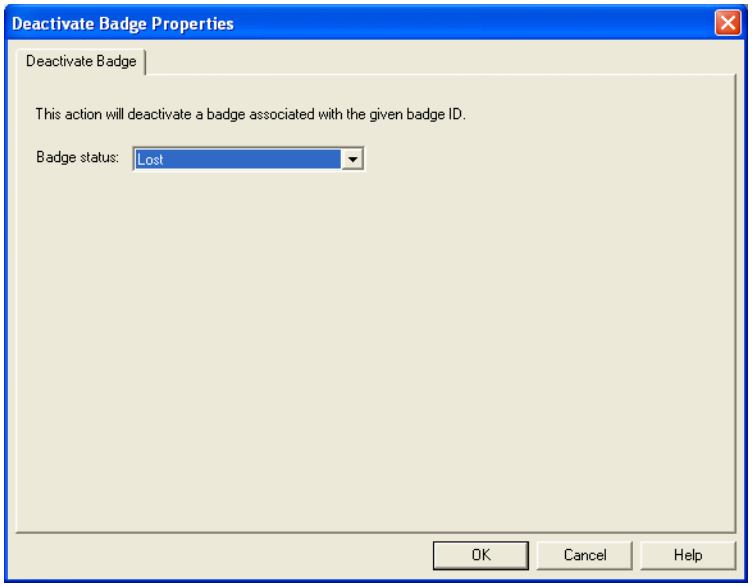
1. Open the DataExchange Script Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) a configuration in the Configuration Name listing window.
3. Click [OK].

Deactivate Badge Properties Window

The Deactivate Badge action allows you to deactivate a cardholder's badge when it is either lost or returned.

You can display the Deactivate Badge Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 1194.

Note: In segmented systems, the Action History/Guard Tour Event Purging action must be applied to all segments.



Badge Status
Use to select the status of a badge that will be deactivated. Choices are Lost and Returned.

OK
Click this button to add the action and exit out of the Deactivate Badge Properties window.

Cancel
Click this button to exit the Deactivate Badge Properties window without adding the action.

Help
Click this button to display online help for this window.

Deactivate Badge Properties Window Procedures

The following procedures can be performed on this form.

Add a Deactivate Badge Action

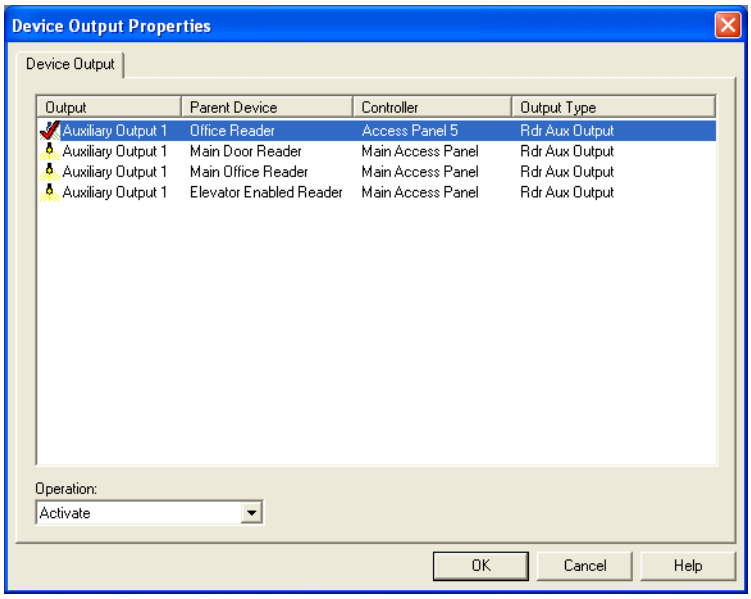
1. Open the Deactivate Badge Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 1194.

Note: In order to execute the action, Global I/O should have a linkage configured on a device, event, and badge ID that is passed to the action at runtime.

2. Click [Add].
3. Click the Output Action sub-tab.
4. Click [Add]. The Add Action Wizard window opens.
5. Select “Deactivate Badge” from the Objects listing window.
6. Click [Next]. The Deactivate Badge Properties window appears.
7. Choose the type of badge you want to deactivate.
8. Click [OK].
9. Click [OK] again.

Device Output Properties Window

You can display the Device Output Properties window using Action Group Library, Scheduler, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Output listing window
Displays a list of available device outputs which have been configured in the system.

Activate
When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will activate. When a device output is activated, that means it is in an “on” state.

Deactivate
When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will deactivate. When a device output is deactivated, that means it is in an “off” state.

Pulse
When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will pulse (turn on and then turn off again).

Toggle
When configuring a device output as an action, select this from the drop-down menu if you want to toggle the state of the relay. For example, if the relay is on (activated), toggling deactivates it. If the relay is off (deactivated), toggling activates it.

Note: Only offboard relays on the Bosch (7412 and 9412) intrusion panels support the toggle option.

OK
Click this button to add the action and exit out of the Device Output Properties window.

Cancel
Click this button to exit the Device Output Properties window without adding the action.

Help
Click this button to display online help for this window.

Device Output Properties Window Procedures

The following procedures can be performed on this form.

Add a Device Output Action

1. Open the Device Output Properties window using the Action Group Library, Scheduler, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) an entry in the Output listing window.
3. Do one of the following:
   - Select **Activate** from the drop-down if you want this action to be that the device output will activate. When a device output is activated, that means it is in an “on” state.
   - Select **Deactivate** from the drop-down if you want this action to be that the device output will deactivate. When a device output is deactivated, that means it is in an “off’ state.

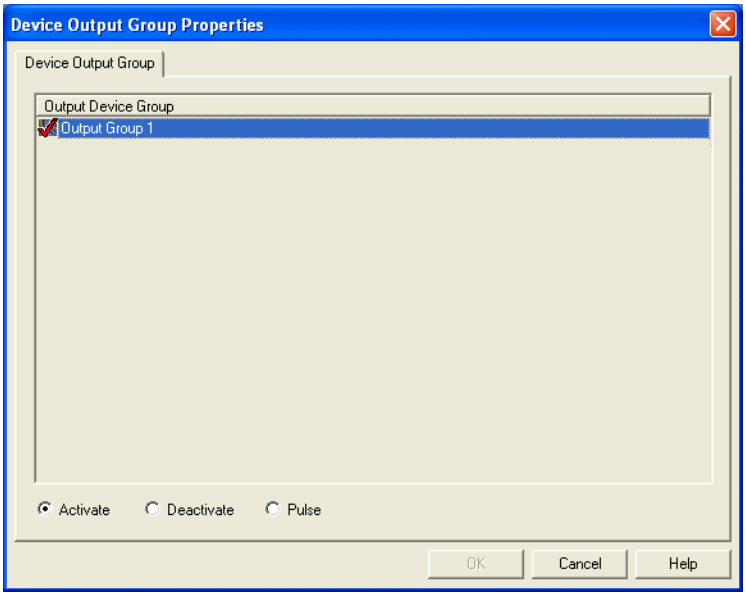
- Select **Pulse** from the drop-down if you want this action to be that the device output will pulse (turn on and then turn off again).
- Select **Toggle** from the drop-down in you want this action to be that the device output will toggle the state of the relay. For example, if the relay is on (activated), toggling deactivates it. If the relay is off (deactivated), toggling activates it.

Note: Only offboard relays on the Bosch (7412 and 9412) intrusion panels support the toggle option.

4. Click [OK].

Device Output Group Properties Window

You can display the Device Output Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Output Device Group listing window

Displays a list of available output device groups which have been configured in the system.

Activate

When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will activate. When device outputs are activated, that means they are in an “on” state.

Deactivate

When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will deactivate. When device outputs are deactivated, that means they are in an “off” state.

Pulse

When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will pulse (they will turn on and then turn off again).

OK

Click this button to add the action and exit out of the Device Output Group Properties window.

Cancel

Click this button to exit the Device Output Group Properties window without adding the action.

Help

Click this button to display online help for this window.

Device Output Group Properties Window Procedures

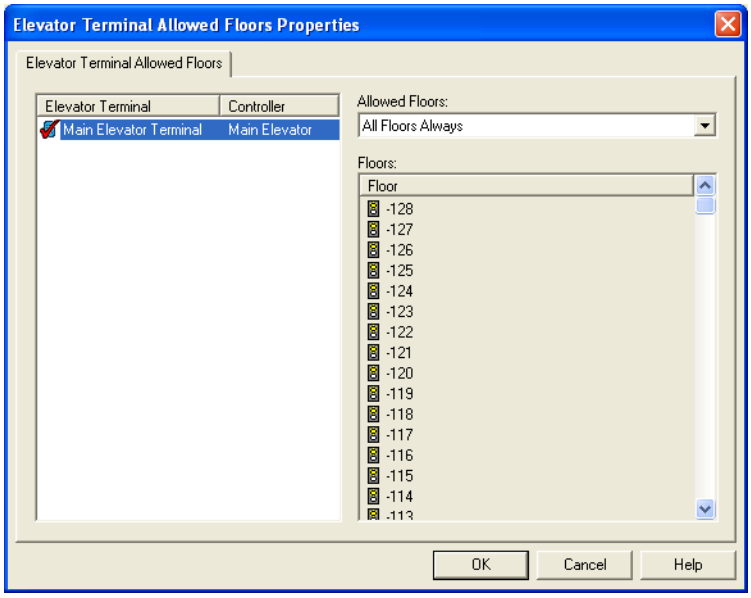
The following procedures can be performed on this form.

Add a Device Output Group Action

1. Open the Device Output Group Properties window, using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) a group in the Output Device Group listing window.
3. Do one of the following:
   - Select the **Activate** radio button if you want this action to be that the device outputs in the group will activate. When device outputs are activated, that means they are in an “on” state.
   - Select the **Deactivate** radio button if you want this action to be that the device outputs in the group will deactivate. When device outputs are deactivated, that means they are in an “off’ state.
   - Select the **Pulse** radio button if you want this action to be that the device outputs in the group will pulse (they will turn on and then turn off again).
4. Click [OK].

Elevator Terminal Allowed Floors Properties Window

You can display the Elevator Terminal Allowed Floors Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Allowed Floors

Allowed floors are floors that can be accessed via the elevator terminal without supplying security credentials. Your options include:

- **All Floors Always** - the elevator is allowed to all floors no matter the security credentials presented.
- **No Floors** - The elevator is allowed to no floors without security credentials being presented.

Floors

Lists the floors the elevator is capable of traveling to.

Elevator Terminal Allowed Floors Properties Window Procedures

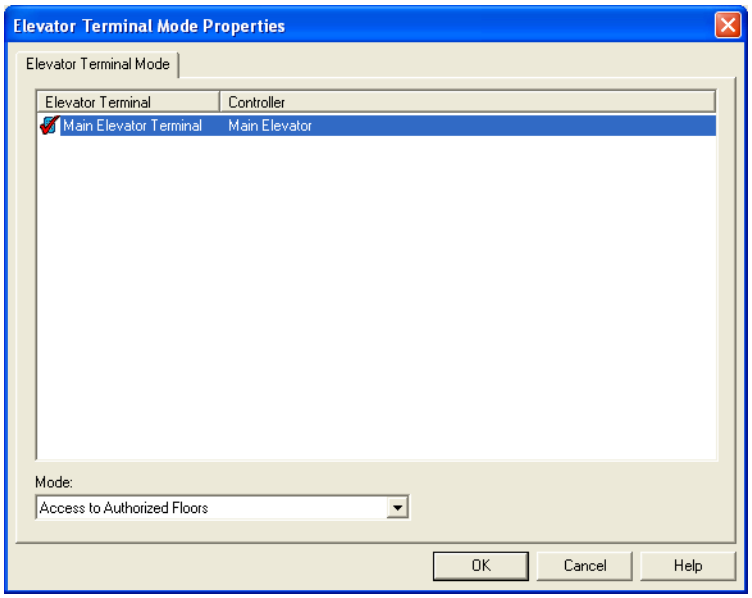
The following procedures can be performed on this form.

Add an Elevator Terminal Allowed Floors Action

1. Open the Elevator Terminal Allowed Floors Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Select an elevator terminal in the listing window.
3. Select an option in the **Allowed Floors** drop-down.
4. Click [OK].

Elevator Terminal Mode Properties Window

You can display the Elevator Terminal Mode Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Elevator Terminal Mode listing window

Lists the current elevator terminals and elevator controllers.

Mode

Refers to operational modes which dictate how the terminal interacts with the cardholder. Choose from:

- Access to Authorized Floors
- Default Floor Only
- Default Floor or User Entry of Destination Floor
- User Entry of Destination Floor

Elevator Terminal Mode Properties Window Procedures

The following procedures can be performed on this form.

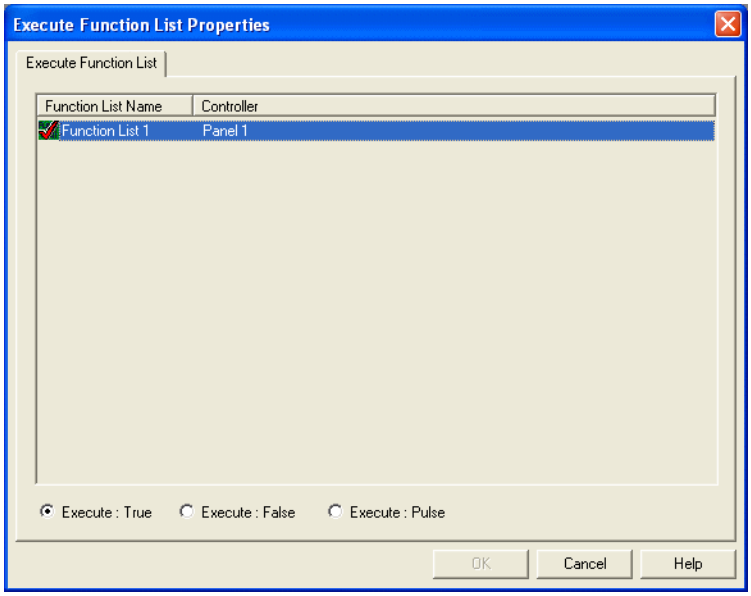
Add an Elevator Terminal Mode Action

1. Open the Elevator Terminal Mode Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Select an elevator terminal in the listing window.

3. Select an option in the **Mode** drop-down.
4. Click [OK].

Execute Function List Properties Window

You can display the Execute Function List Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Function List listing window

Displays a list of available function lists which have been configured in the system.

Execute: True

When configuring a function list as an action, select this radio button if you want the action to execute the function list with an argument of “True.”

Execute: False

When configuring a function list as an action, select this radio button if you want the action to execute the function list with an argument of “False.”

Execute: Pulse

When configuring a function list an action, select this radio button if you want the action to execute the function list with an argument of “Pulse.”

OK

Click this button to add the action and exit out of the Execute Function List Properties window.

Cancel
Click this button to exit the Execute Function List Properties window without adding the action.

Help
Click this button to display online help for this window.

Execute Function List Properties Window Procedures

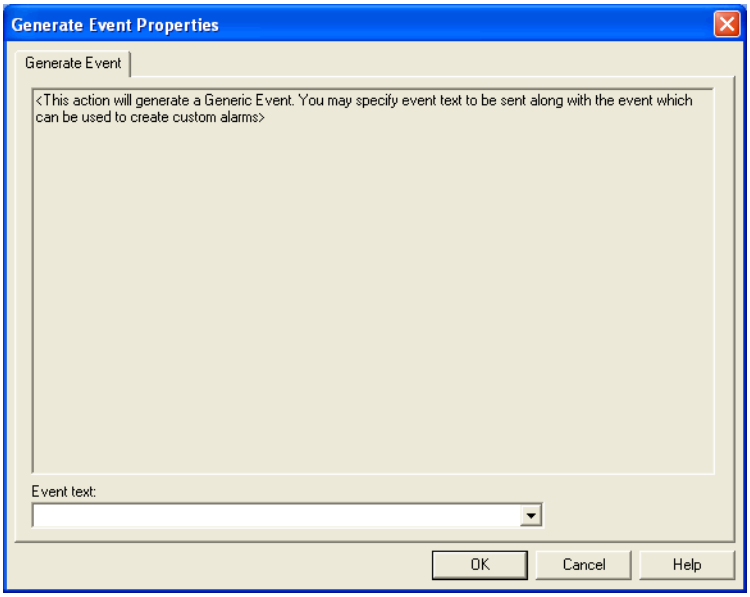
The following procedures can be performed on this form.

Add an Execute Function List Action

1. Open the Execute Function List Properties window, using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) an entry in the Function List listing window.
3. Do one of the following:
   - Select the **Execute: True** radio button if you want this action to execute the function list with an argument of “True.”
   - Select the **Execute: False** radio button if you want this action to execute the function list with an argument of “False.”
   - Select the **Execute: Pulse** radio button if you want this action to execute the function list with an argument of “Pulse.”
4. Click [OK].

Generate Event Properties Window

You can display the Generate Event Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.



Event text
Type your custom event text here. You must create your own event text for this event.

OK
Click this button to add the action and exit out of the window.

Cancel
Click this button to exit the window without adding the action.

Help
Click this button to display online help for this window.

Elevator Terminal Mode Properties Window Procedures

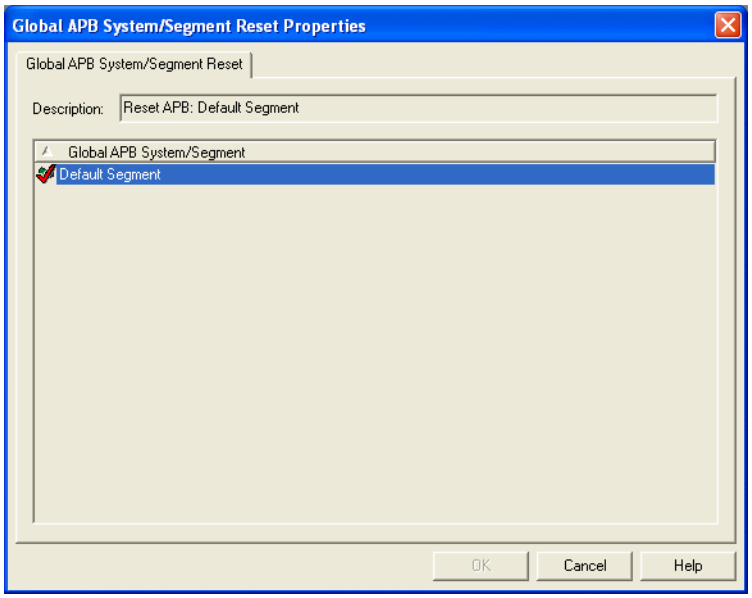
The following procedures can be performed on this form.

Add an Elevator Mode Action

1. Open the Elevator Terminal Mode Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Select an elevator terminal in the listing window.
3. Select an option in the **Mode** drop-down.
4. Click [OK].

Global APB System/Segment Reset Properties Window

You can display the Global APB System/Segment Reset Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.



Description
Displays a description of the selected global APB system/segment.

Global APB System/Segment listing window
Displays a list of the segments available for this action.

OK
Click this button to add the action and exit out of the Global APB System/Segment Reset Properties window.

Cancel
Click this button to exit the Global APB System/Segment Reset Properties window without adding the action.

Help
Click this button to display online help for this window.

Global APB System/Segment Reset Properties Window Procedures

The following procedures can be performed on this form.

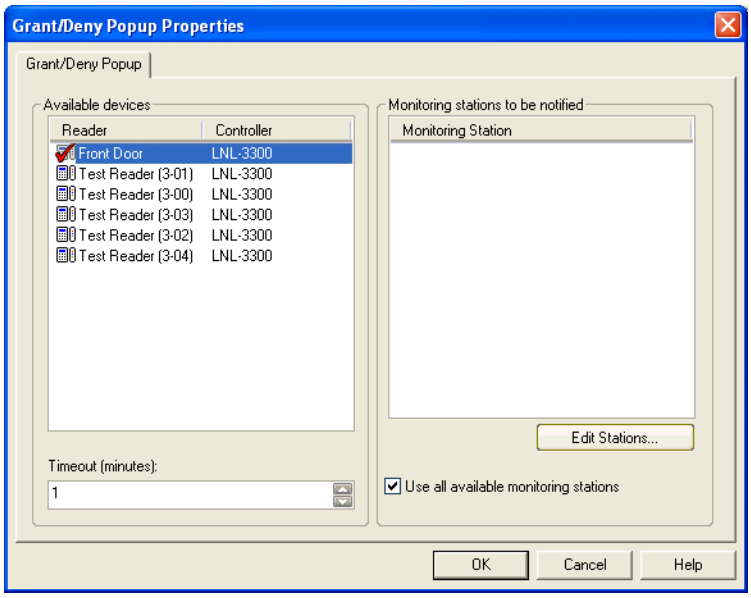
Add a Global APB System/Segment Reset Action

Note: Global APB must be configured on your system in order to add this action.

1. Open the Global APB System/Segment Reset Properties window, using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) a segment from the Global APB System/Segment listing window.
3. Click [OK]. If segmentation is enabled, this action will reset APB for the selected segment. If segmentation is not enabled, this action will reset APB for your entire system.

Grant/Deny Popup Properties Window

You can display the Grant/Deny Popup Properties window using the Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Available devices listing window

Displays a list of readers that are available for selection and the controllers that are associated with each.

Timeout (minutes)

When a grant/deny popup action is executed, a notification is displayed in Alarm Monitoring. The notification informs the Alarm Monitoring operator that a request has been made to access a door. The operator will then have the ability to issue a grant (open door request) or a deny.

In this field, enter the number of minutes that you want the grant/deny popup notification to be displayed in Alarm Monitoring.

You can enter a minimum of 1 and a maximum of 60 minutes.

Monitoring stations to be notified listing window

Displays a list of monitoring stations that are available for selection.

Edit Stations
Click to open the Select Monitoring Stations To Be Notified window. Here you can select specific monitoring stations to be notified instead of all monitoring stations.

Use all available monitoring stations
Enable to notify all available monitoring stations in the database.

OK
Click this button to add the action and exit out of the Grant/Deny Popup Properties window.

Cancel
Click this button to exit the Grant/Deny Popup Properties window without adding the action.

Help
Click this button to display online help for this window.

Grant/Deny Popup Properties Window Procedures

The following procedures can be performed on this form.

Add a Grant/Deny Popup Action

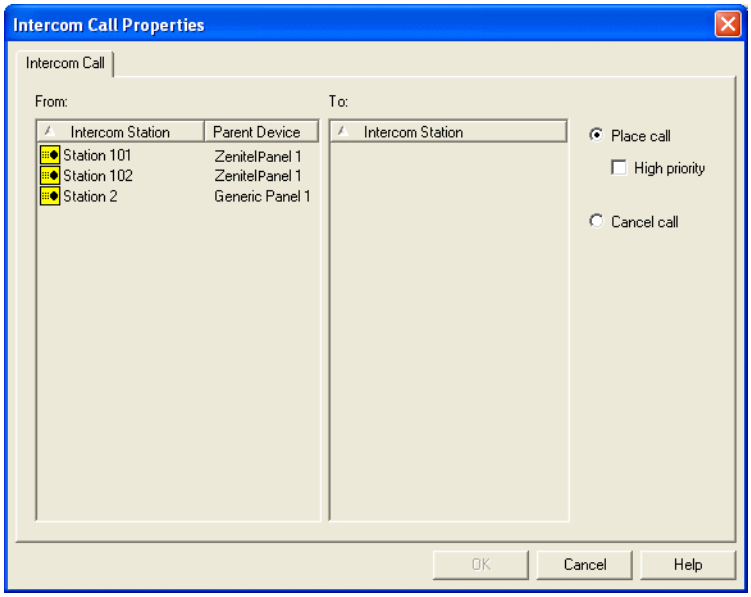
1. Open the Grant/Deny Popup Properties window, using the Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. When a grant/deny popup action is executed, a notification is displayed in Alarm Monitoring. The notification informs the Alarm Monitoring operator that a request has been made to access a door. The operator will then have the ability to issue a grant (open door request) or a deny. From the Reader/Controller listing window, select the door that you want to configure for this grant/deny popup action.
3. In the Timeout (minutes) field, enter the number of minutes that you want the grant/deny popup notification to be displayed in Alarm Monitoring. You can enter a minimum of 1 and a maximum of 60 minutes.
4. In the Monitoring stations to be notified listing window select the monitoring stations to be notified of a grant/deny popup action.
   a. Click [Edit Stations] to select specific monitoring stations or select the **Use all available monitoring stations** check box to select all of the monitoring stations.
5. Click [OK].

Intercom Call Properties Window

You can display the Intercom Call Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 1194.

The Intercom Call action is available from the Global I/O only. If you create an action group that includes the Intercom Call action, you will not be able to add this group to the Scheduler, Guard tour, or Acknowledgment Actions. This group can only be added to the Global I/O.

Note: In order to execute the action, Global I/O should have a linkage configured on a device, event, and badge ID that is passed to the action at runtime.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

From listing window

Displays a list of available intercom stations which have been configured in the system.

To listing window

Lists the intercom stations that have the same parent device as the intercom station which is selected in the From listing window. This field is only enabled when the **Place call** radio button is selected.

Place call

When configuring an intercom call as an action, select this radio button if you want the action to place an intercom call.

High priority

When configuring an intercom call as an action, select this check box if you want the action to be a high priority. This field is only enabled when the **Place call** radio button is selected.

Cancel call

When configuring an intercom call as an action, select this radio button if you want the action to cancel a call.

OK

Click this button to add the action and exit out of the Intercom Call Properties window.

Cancel

Click this button to exit the Intercom Call Properties window without adding the action.

Help

Click this button to display online help for this window.

Intercom Call Properties Window Procedures

The following procedures can be performed on this form.

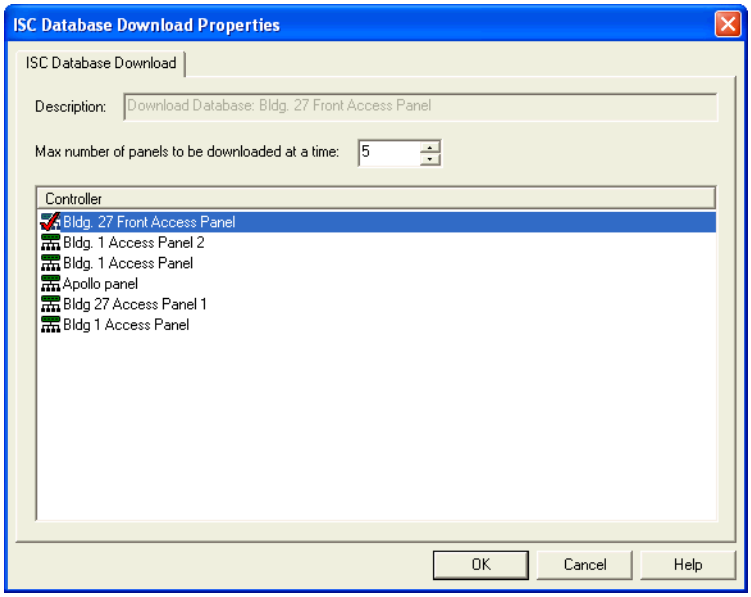
Add an Intercom Call Action

The Intercom Call action is available from the Global I/O only. If you create an action group that includes the Intercom Call action, you will not be able to add this group to the Scheduler or Guard tour.

1. Open the Intercom Call Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) an intercom station in the From listing window. This is the intercom station where the call will be sent from.
3. If you want the action to place a call:
   a. Select the **Place call** radio button if you want this action to place an intercom call.
   b. Select the **High priority** check box if you want this action to be a high priority.
4. If you want the action to cancel a call:
   a. Select the **Cancel call** radio button.
   b. Proceed to step 5.
5. Click on an intercom station in the To listing window to select it. This is the intercom station where the call will be received.
6. Click [OK].

ISC Database Download Properties Window

You can display the ISC Database Download Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Description
Displays a description of the access panel which is selected in the Access Panel listing window.

Note: This field only displays a description when one and only one access panel is selected.

Max number of panels to be downloaded at a time
When configuring a database download as an action, select the maximum number of access panels that can be downloaded at a time.

Controller listing window
Displays a list of available controllers that have been configured in the system.

OK
Click this button to add the action and exit out of the ISC Database Download Properties window.

Cancel
Click this button to exit the ISC Database Download Properties window without adding the action.

Help
Click this button to display online help for this window.

ISC Database Download Properties Window Procedures

The following procedures can be performed on this form.

Add an ISC Database Download Action

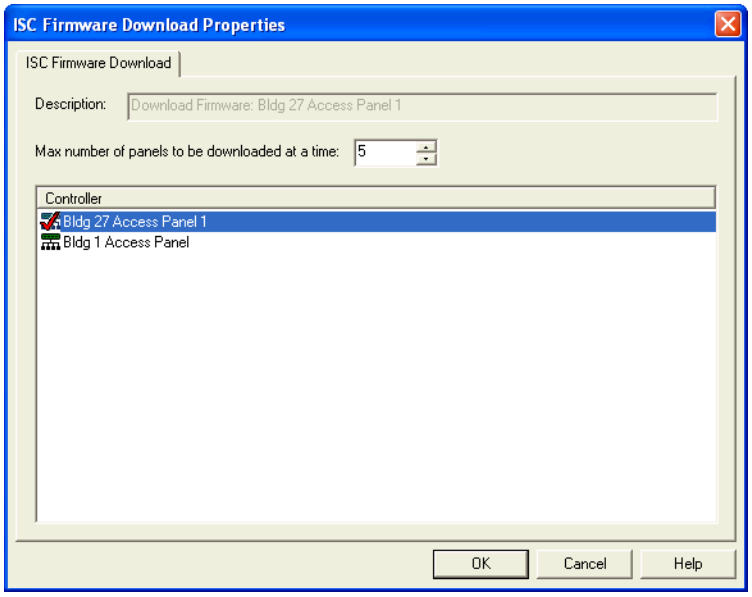
1. Open the ISC Database Download Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Select the **max number of panels to be downloaded at a time**.
3. From the Access Panel listing window, click on an entry to select it.

Note: You can select multiple entries.

4. Click [OK].

ISC Firmware Download Properties Window

You can display the ISC Firmware Download Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Description

Displays a description of the access panel which is selected in the Access Panel listing window.

Note: This field only displays a description when one and only one access panel is selected.

Max number of panels to be downloaded at a time

When configuring a firmware download as an action, select the maximum number of access panels that can be downloaded at a time.

Controller listing window

Displays a list of available controllers that have been configured in the system.

OK
Click this button to add the action and exit out of the ISC Firmware Download Properties window.

Cancel
Click this button to exit the ISC Firmware Download Properties window without adding the action.

Help
Click this button to display online help for this window.

ISC Firmware Download Properties Window Procedures

The following procedures can be performed on this form.

Add an ISC Firmware Download Action

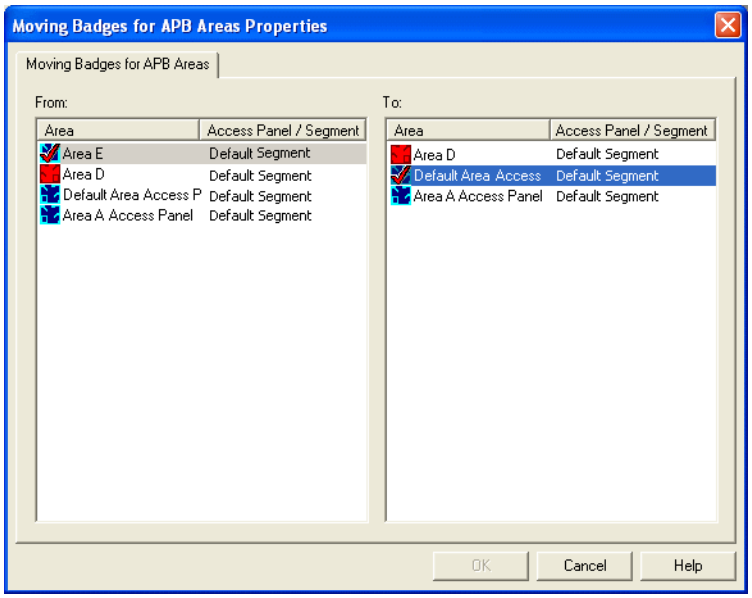
1. Open the ISC Firmware Download Properties window, using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. Select the **max number of panels to be downloaded at a time**.
3. From the Access Panel listing window, click on an entry to select it.

Note: You can select multiple entries.

4. Click [OK].

Moving Badges for APB Areas Properties Window

You can display the Moving Badges for APB Areas Properties window using Action Group Library, Scheduler, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

From listing window

Displays a list of areas that are available for selection.

To listing window

Displays a list of areas that are available for selection.

OK

Click this button to add the action and exit out of the Moving Badges for APB Areas Properties window.

Cancel

Click this button to exit the Moving Badges for APB Areas Properties window without adding the action.

Help

Click this button to display online help for this window.

Moving Badges for APB Areas Properties Window Procedures

The following procedures can be performed on this form.

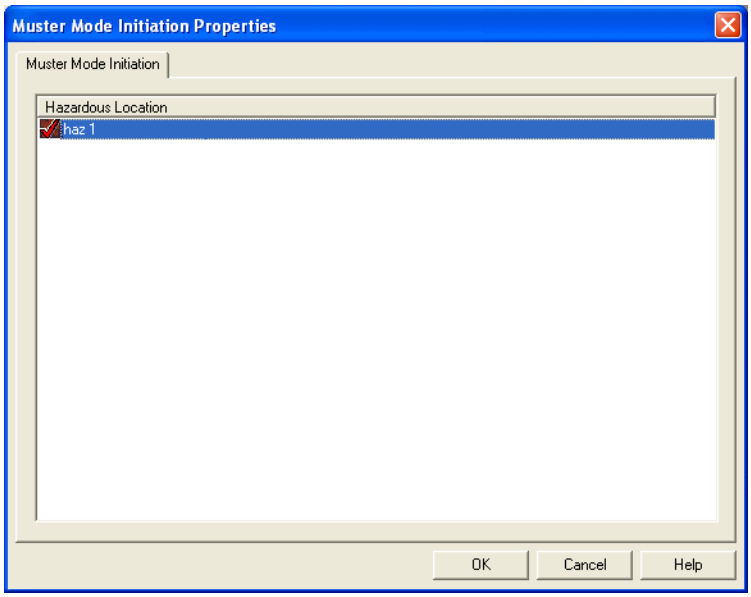
Add a Moving Badges for APB Areas Action

1. Open the Moving Badges for APB Areas Properties window using the Action Group Library, Scheduler, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.

2. In the From listing window, select (place a checkmark beside) the area that you want to move badges from when this action is executed.
3. In the To listing window, select (place a checkmark beside) the area that you want to move badges to when this action is executed.
4. Click [OK].

Muster Mode Initiation Properties Window

You can display the Muster Mode Initiation Properties window using the Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Hazardous Location listing window
Displays a list of available hazardous locations that have been configured in the system.

OK
Click this button to add the action and exit out of the Muster Mode Initiation Properties window.

Cancel
Click this button to exit the Muster Mode Initiation Zone Properties window without adding the action.

Help
Click this button to display online help for this window.

Muster Mode Initiation Properties Window Procedures

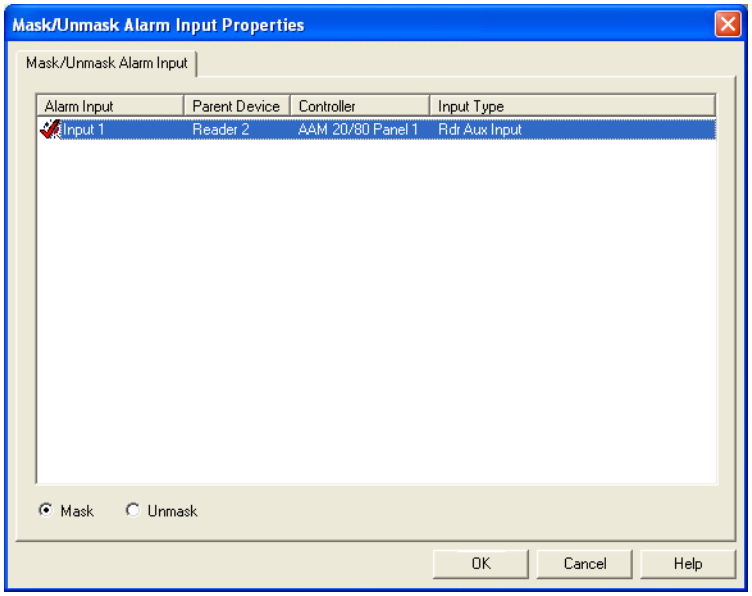
The following procedures can be performed on this form.

Add a Muster Mode Initiation Action

1. Open the Muster Mode Initiation Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. From the listing window, click on an entry to select it.
3. Click [OK]. This action is now configured to initiate muster mode in the selected hazardous location. (Refer to the Areas folder chapter in this user guide for more information on mustering.)

Mask/Unmask Alarm Input Properties Window

You can display the Mask/Unmask Alarm Input Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Alarm Input listing window

Displays a list of available alarm inputs which have been configured in the system.

Mask

When configuring a mask/unmask alarm input action, select this radio button if you want the alarm input to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.

Unmask

When configuring a mask/unmask alarm input action, select this radio button if you want the alarm input to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.

OK
Click this button to add the action and exit out of the Mask/Unmask Alarm Input Properties window.

Cancel
Click this button to exit the Mask/Unmask Alarm Input Properties window without adding the action.

Help
Click this button to display online help for this window.

Mask/Unmask Alarm Input Properties Window Procedures

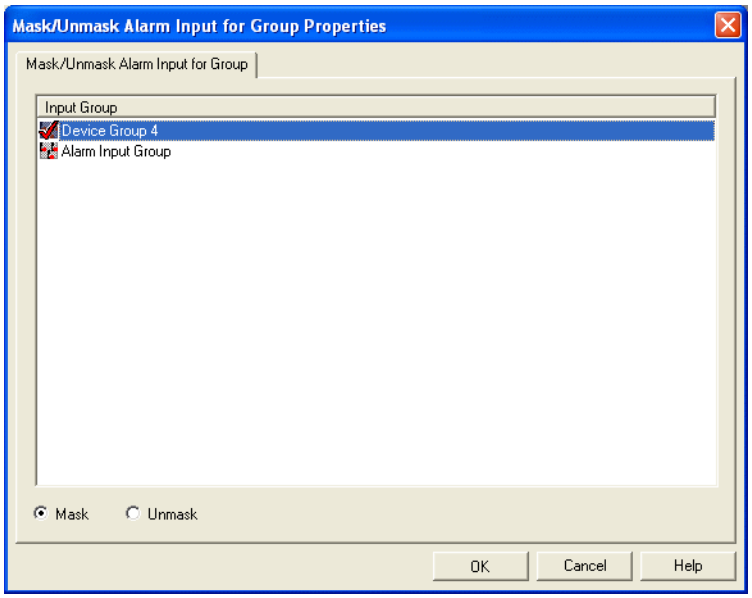
The following procedures can be performed on this form.

Add a Mask/Unmask Alarm Input Action

1. Open the Mask/Unmask Alarm Input Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. From the Alarm Input listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want the alarm input to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the alarm input to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Alarm Input for Group Properties Window

You can display the Mask/Unmask Alarm Input for Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Input Group listing window

Displays a list of available alarm input groups which have been configured in the system.

Mask

When configuring a mask/unmask alarm input for group action, select this radio button if you want the group of alarm inputs to be masked. When alarm input groups are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.

Unmask

When configuring a mask/unmask alarm input for group action, select this radio button if you want the group of alarm inputs to be unmasked. When alarm input groups are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.

OK

Click this button to add the action and exit out of the Mask/Unmask Alarm Input for Group Properties window.

Cancel

Click this button to exit the Mask/Unmask Alarm Input for Group Properties window without adding the action.

Help

Click this button to display online help for this window.

Mask/Unmask Alarm Input for Group Properties Window Procedures

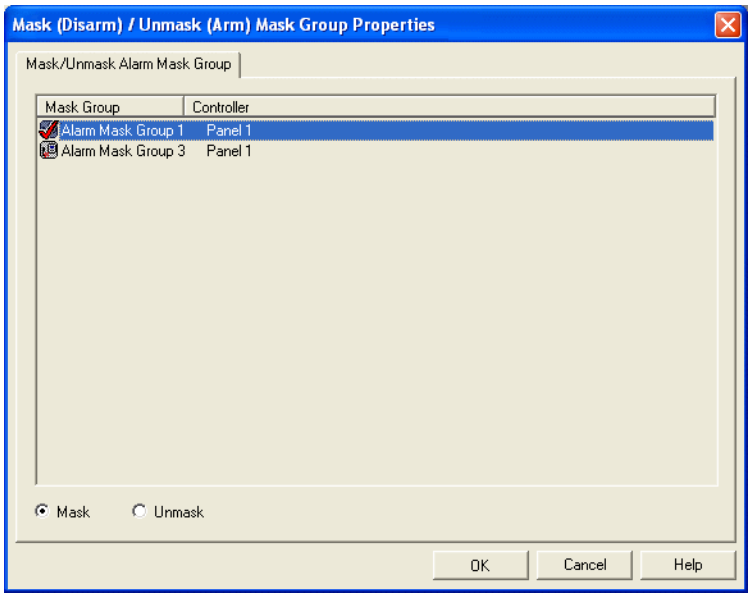
The following procedures can be performed on this form.

Add a Mask/Unmask Alarm Input for Group Action

1. Open the Mask/Unmask Alarm Input for Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. From the Input Group listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want the alarm inputs in the group to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the alarm inputs in the group to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask (Disarm)/Unmask (Arm) Mask Group Properties Window

You can display the Mask/Unmask Alarm Mask for Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Mask Group listing window
Displays a list of available alarm mask groups which have been configured in the system.

Mask
When configuring a Mask (Disarm) / Unmask (Arm) Mask Group action, select this radio button if you want the mask group to be masked. When alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.

Unmask
When configuring a Mask (Disarm) / Unmask (Arm) Mask Group action, select this radio button if you want the mask group to be unmasked. When alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.

OK
Click this button to add the action and exit out of the Mask (Disarm) / Unmask (Arm) Mask Group Properties window.

Cancel
Click this button to exit the Mask (Disarm) / Unmask (Arm) Mask Group Properties window without adding the action.

Help
Click this button to display online help for this window.

Mask (Disarm)/Unmask (Arm) Mask Group Properties Window Procedures

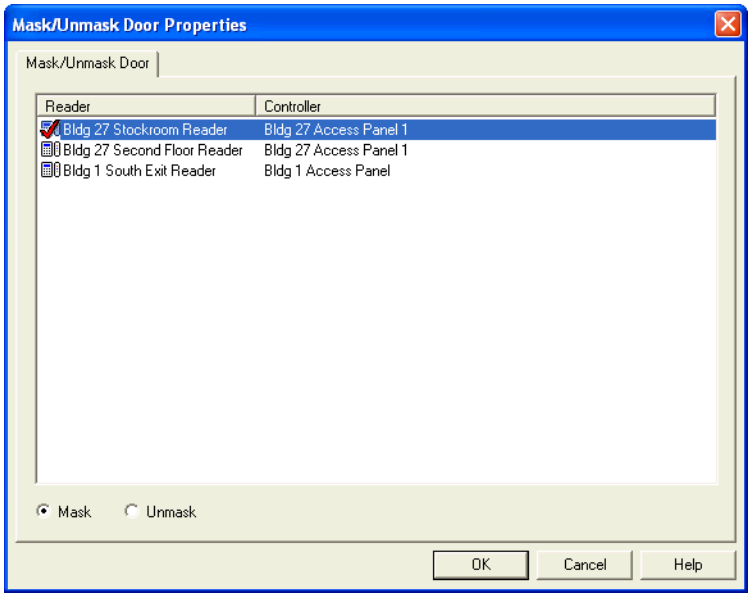
The following procedures can be performed on this form.

Add a Mask (Disarm)/Unmask (Arm) Mask Group Action

1. Open the Mask/Unmask Alarm Mask for Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) and entry in the Mask Group listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want the mask group to be masked. When alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the mask group to be unmasked. When alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Properties Window

You can display the Mask/Unmask Door Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader/Controller listing window

Displays a list of readers that are available for selection and the controllers that are associated with each.

Mask

When configuring a mask/unmask door action, select this radio button if you want the action to be that the door is masked. When masked doors generate alarms, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.

Unmask

When configuring a mask/unmask door action, select this radio button if you want the action to be that the door is unmasked. When unmasked doors generate alarms, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.

OK

Click this button to add the action and exit out of the Mask/Unmask Door Properties window.

Cancel

Click this button to exit the Mask/Unmask Door Properties window without adding the action.

Help

Click this button to display online help for this window.

Mask/Unmask Door Properties Window Procedures

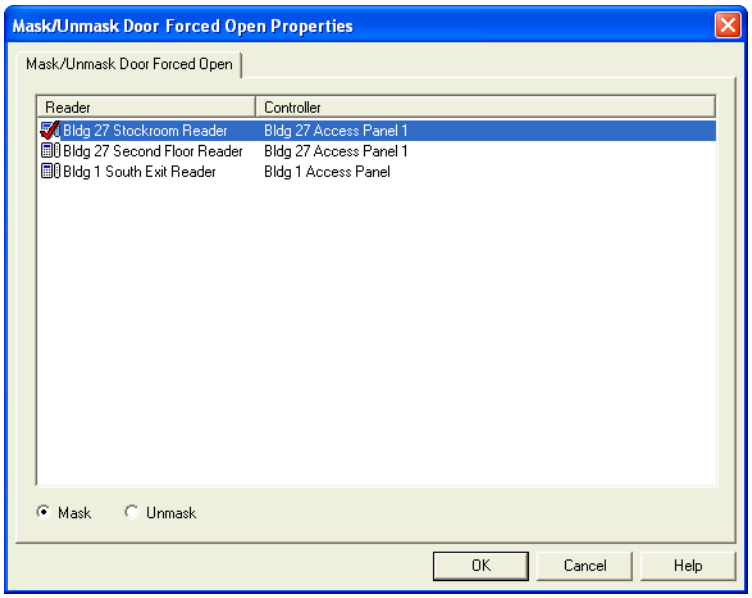
The following procedures can be performed on this form.

Add a Mask/Unmask Door Action

1. You can display the Mask/Unmask Door Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) and entry in the Reader/Controller listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want the action to be that the door is masked. When masked doors generate alarms, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the action to be that the door is unmasked. When unmasked doors generate alarms, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Forced Open Properties Window

You can display the Mask/Unmask Door Forced Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader/Controller listing window
Displays a list of available readers which have been configured in the system and the controllers that are associated with each.

Mask
When configuring a mask/unmask door forced open action, select this radio button if you want the door forced open alarm to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.

Unmask
When configuring a mask/unmask door forced open action, select this radio button if you want the door forced open alarm to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.

OK
Click this button to add the action and exit out of the Mask/Unmask Door Forced Open Properties window.

Cancel
Click this button to exit the Mask/Unmask Door Forced Open Properties window without adding the action.

Help
Click this button to display online help for this window.

Mask/Unmask Door Forced Open Properties Window Procedures

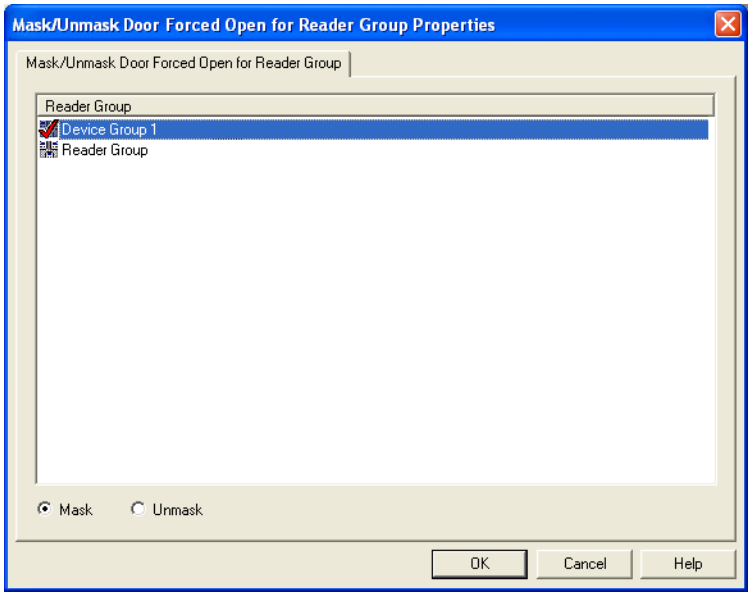
The following procedures can be performed on this form.

Add a Mask/Unmask Door Forced Open Action

1. Open the Mask/Unmask Door Forced Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) and entry in the Reader/Controller listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want door forced open alarms for the selected reader to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door forced open alarms for the selected reader to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Forced Open for Reader Group Properties Window

You can display the Mask/Unmask Door Forced Open for Reader Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader Group listing window

Displays a list of available reader groups which have been configured in the system.

Mask

When configuring a mask/unmask door forced open for reader group action, select this radio button if you want the door forced open alarms to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.

Unmask

When configuring a mask/unmask door forced open for reader group action, select this radio button if you want the door forced open alarms to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.

OK

Click this button to add the action and exit out of the Mask/Unmask Door Forced Open for Reader Group Properties window.

Cancel

Click this button to exit the Mask/Unmask Door Forced Open for Reader Group Properties window without adding the action.

Help

Click this button to display online help for this window.

Mask/Unmask Door Forced Open for Reader Group Properties Window Procedures

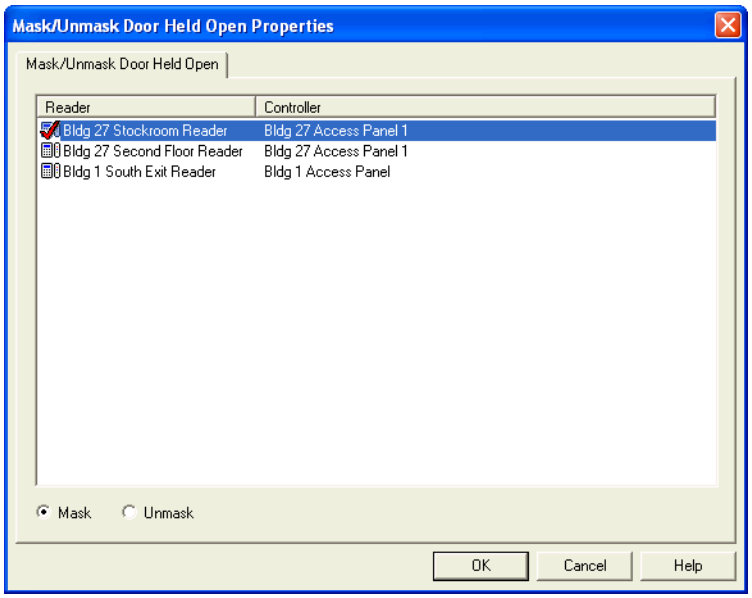
The following procedures can be performed on this form.

Add a Mask/Unmask Door Forced Open for Reader Group Action

1. Open the Mask/Unmask Door Forced Open for Reader Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) and entry in the Reader Group listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want door forced open alarms for the selected reader group to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door forced open alarms for the selected reader group to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Held Open Properties Window

You can display the Mask/Unmask Door Held Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader/Controller listing window

Displays a list of available readers which have been configured in the system and the controllers that are associated with each.

Mask

When configuring a mask/unmask door held open action, select this radio button if you want the door held open alarm to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.

Unmask

When configuring a mask/unmask door held open action, select this radio button if you want the door held open alarm to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.

OK

Click this button to add the action and exit out of the Mask/Unmask Door Held Open Properties window.

Cancel

Click this button to exit the Mask/Unmask Door Held Open Properties window without adding the action.

Help

Click this button to display online help for this window.

Mask/Unmask Door Held Open Properties Window Procedures

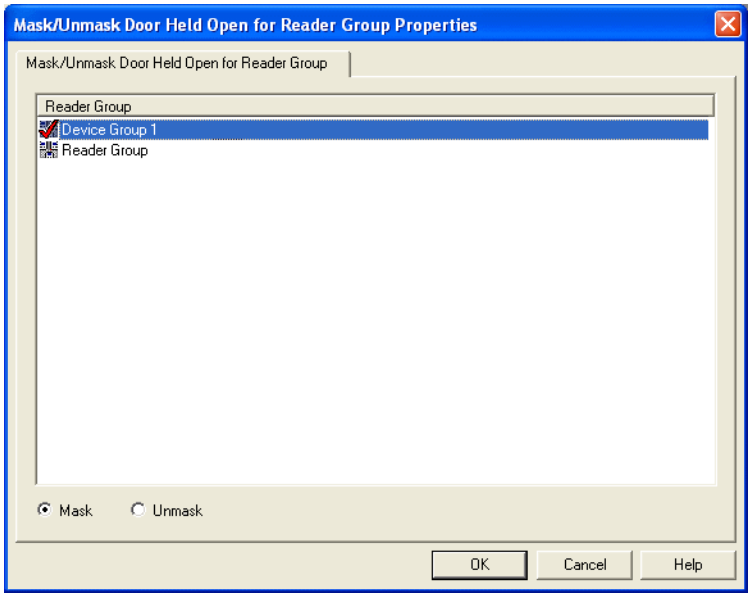
The following procedures can be performed on this form.

Add a Mask/Unmask Door Held Open Action

1. Open the Mask/Unmask Door Held Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) and entry in the Reader/Controller listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want door held open alarms for the selected reader to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door held open alarms for the selected reader to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Held Open for Reader Group Properties Window

You can display the Mask/Unmask Door Held Open for Reader Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader Group listing window

Displays a list of available reader groups which have been configured in the system.

Mask

When configuring a mask/unmask door held open for reader group action, select this radio button if you want the door held open alarms to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.

Unmask

When configuring a mask/unmask door held open for reader group action, select this radio button if you want the door held open alarms to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.

OK

Click this button to add the action and exit out of the Mask/Unmask Door Held Open for Reader Group Properties window.

Cancel

Click this button to exit the Mask/Unmask Door Held Open for Reader Group Properties window without adding the action.

Help

Click this button to display online help for this window.

Mask/Unmask Door Held Open for Reader Group Properties Window Procedures

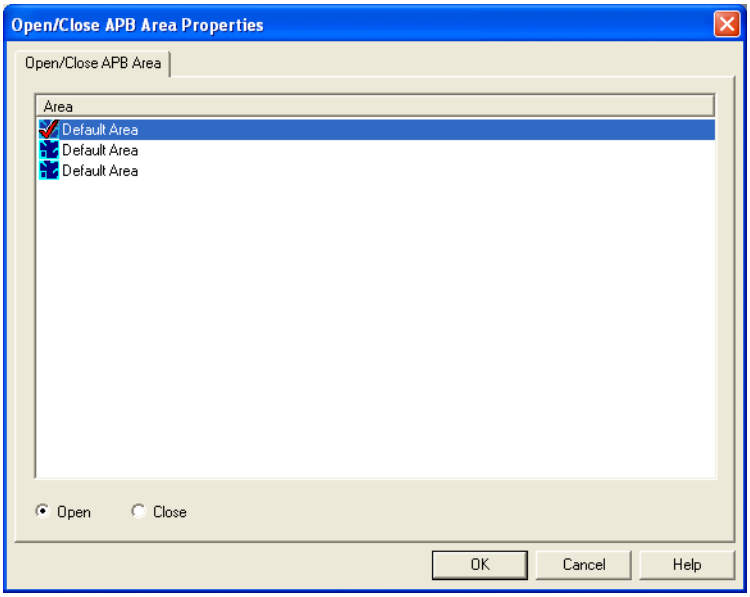
The following procedures can be performed on this form.

Add a Mask/Unmask Door Held Open for Reader Group Action

1. Open the Mask/Unmask Door Held Open for Reader Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. From the Reader Group listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want door held open alarms for the selected reader group to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door held open alarms for the selected reader group to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Open/Close APB Area Properties Window

You can display the Mask/Unmask Door Held Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Area listing window
Displays a list of areas that are available for selection.

Open
When configuring an open/close APB area action, select this radio button if you want the action to be that the APB area opens.

Close
When configuring an open/close APB area action, select this radio button if you want the action to be that the APB area closes.

OK
Click this button to add the action and exit out of the Open/Close APB Area Properties window.

Cancel
Click this button to exit the Open/Close APB Area Properties window without adding the action.

Help
Click this button to display online help for this window.

Open/Close APB Area Properties Window Procedures

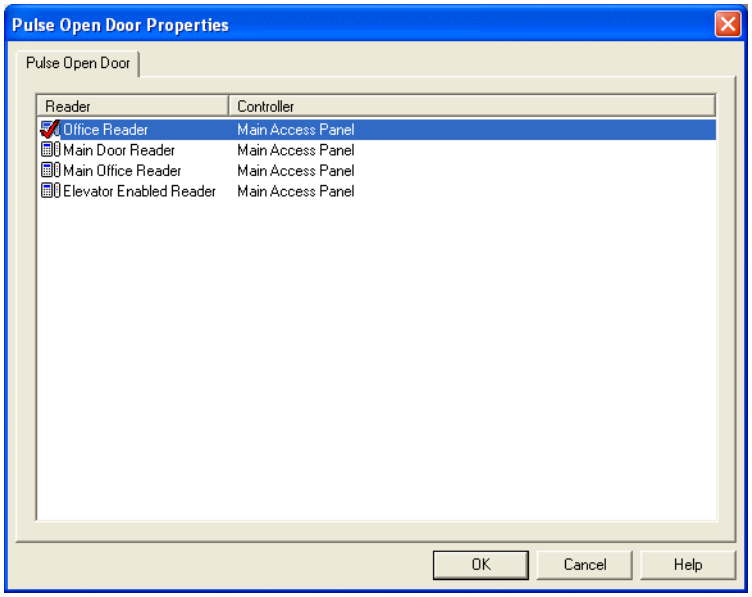
The following procedures can be performed on this form.

Add an Open/Close APB Area Action

1. Open the Mask/Unmask Door Held Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select an area from the listing window.
3. Do one of the following:
   - Select the **Open** radio button if you want the action to be that the APB area opens.
   - Select the **Close** radio button if you want the action to be that the APB area closes.
4. Click [OK].

Pulse Open Door Properties Window

You can display the Pulse Open Door Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader/controller listing window

Displays a list of available readers which have been configured in the system and the controllers that are associated with each.

OK
Click this button to add the action and exit out of the Pulse Open Door Properties window.

Cancel
Click this button to exit the Pulse Open Door Properties window without adding the action.

Help
Click this button to display online help for this window.

Pulse Open Door Properties Window Procedures

The following procedures can be performed on this form.

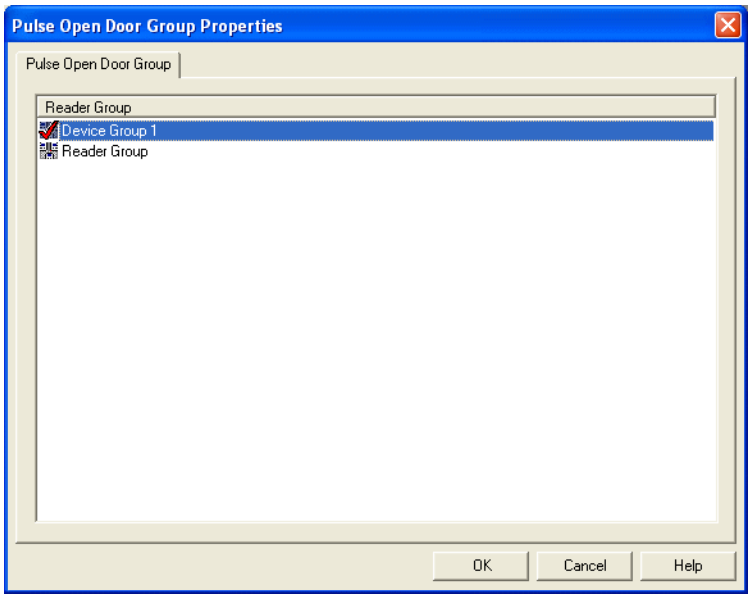
Add a Pulse Open Door Action

Note: The open door commands will not be available for those using Schlage Wireless Access readers, because those types of readers are not in constant communication with the PIM device.

1. Open the Pulse Open Door Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) and entry in the listing window.
3. Click [OK]. The pulse open door action (the door opens and then closes) is now configured for the selected reader.

Pulse Open Door Group Properties Window

You can display the Pulse Open Door Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader Group listing window
Displays a list of available readers groups which have been configured in the system.

OK
Click this button to add the action and exit out of the Pulse Open Door Group Properties window.

Cancel
Click this button to exit the Pulse Open Door Group Properties window without adding the action.

Help
Click this button to display online help for this window.

Pulse Open Door Group Properties Window Procedures

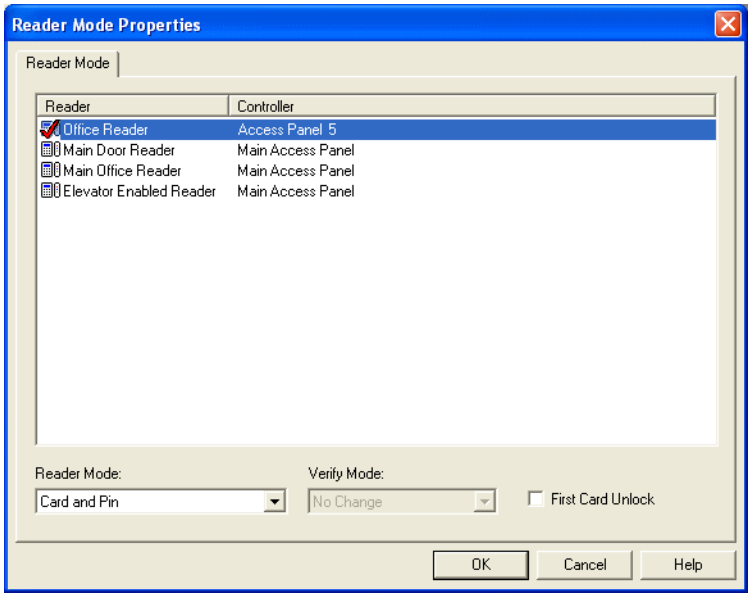
The following procedures can be performed on this form.

Add a Pulse Open Door Group Action

1. Open the Pulse Open Door Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) and entry in the Reader Group listing window.
3. Click [OK]. The pulse open door group action (the doors open and then close) is now configured for the selected reader.

Reader Mode Properties Window

You can display the Reader Mode Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader/Controller listing window

Displays a list of available readers which have been configured in the system and the controllers that are associated with each.

Reader Mode

When configuring a reader mode action, select a mode from this drop-down list. Choices include: Card Only, Facility Code Only, Locked, Card and Pin, Pin or Card, Unlocked, or Default Reader Mode (used to return a reader to its default online access mode).

Verify Mode

When configuring a reader mode action for a reader on a Lenel controller that is a primary reader to an alternate biometric reader, you can select a verify mode. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader. When configuring a reader mode action for a reader that is not a primary reader to an alternate biometric reader, this field is disabled.

First Card Unlock

Select this check box if you want the reader mode action to be that first card unlock mode is enabled. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader

mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.

Note: If the reader is in “Facility code only” mode, the first card unlock feature does not work.

OK
Click this button to add the action and exit out of the Reader Mode Properties window.

Cancel
Click this button to exit the Reader Mode Properties window without adding the action.

Help
Click this button to display online help for this window.

Reader Mode Properties Window Procedures

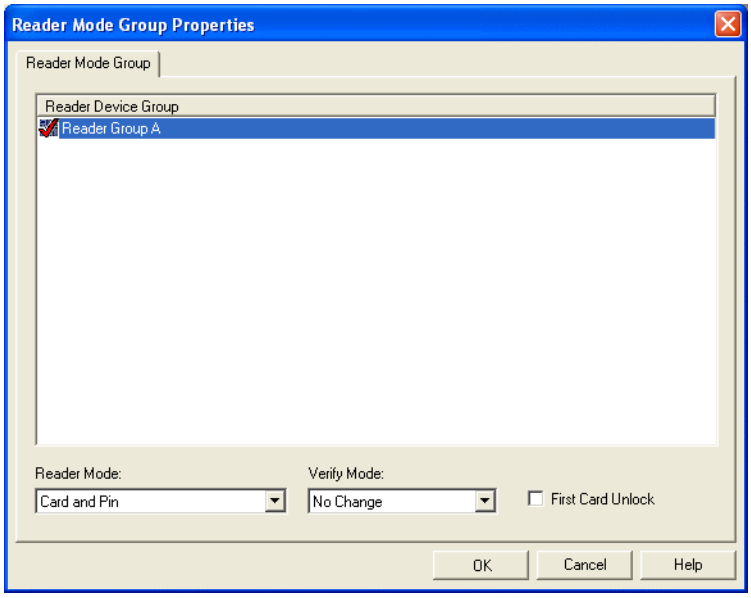
The following procedures can be performed on this form.

Add a Reader Mode Action

1. Open the Reader Mode Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) an entry in the Reader/Controller listing window.
3. From the **Reader Mode** drop-down list, select a reader mode for the selected reader/controller.
4. When configuring a reader mode action for a reader on a Lenel controller that is a primary reader to an alternate biometric reader, you can select a **Verify Mode**. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader.
5. Select the **First Card Unlock** check box if you want this reader mode action to enable first card unlock.
6. Click [OK].

Reader Mode Group Properties Window

You can display the Reader Mode Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Reader Device Group listing window

Displays a list of available reader groups which have been configured in the system.

Reader Mode

When configuring a reader mode action, select a mode from this drop-down list. Choices include: Card Only, Facility Code Only, Locked, Card and Pin, Pin or Card, Unlocked, or Default Reader Mode (used to return a reader to its default online access mode).

Verify Mode

When configuring a reader mode group action for a group of readers on a Lenel controller that are primary readers to alternate biometric readers, you can select a verify mode. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader. When configuring a reader mode group action for readers that are not primary readers alternate biometric readers, this field is disabled.

First Card Unlock

Select this check box if you want the reader mode group action to be that first card unlock mode is enabled. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.

Note: If the reader is in “Facility code only” mode, the first card unlock feature does not work.

OK

Click this button to add the action and exit out of the Reader Mode Group Properties window.

Cancel
Click this button to exit the Reader Mode Group Properties window without adding the action.

Help
Click this button to display online help for this window.

Reader Mode Group Properties Window Procedures

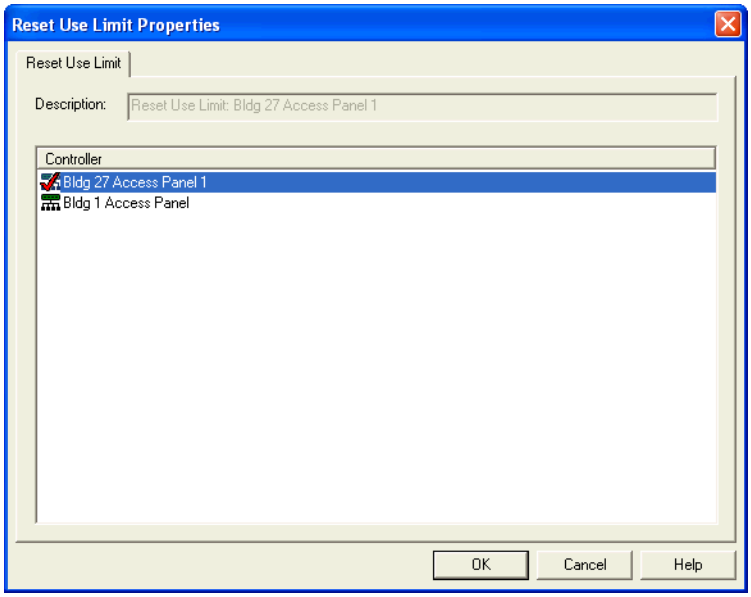
The following procedures can be performed on this form.

Add a Reader Mode Group Action

1. Open the Reader Mode Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) and entry in the Reader Device Group listing window.
3. From the **Reader Mode** drop-down list, select a reader mode for the selected reader group.
4. When configuring a reader mode group action for readers on a Lenel controller that are primary readers to alternate biometric readers, you can select a **Verify Mode**. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader.
5. Select the **First Card Unlock** check box if you want this reader mode group action to enable first card unlock.
6. Click [OK].

Reset Use Limit Properties Window

You can display the Reset Use Limit Properties window using the Action Group Library, Scheduler, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Description

When one controller is selected in the listing window, displays the text "Reset Use Limit:" followed by the controller name. For example, "Reset Use Limit: Front Door Bldg 1." When more than one controller is selected in the listing window, this field is activated. Type in a descriptive name to identify the selected group of controllers.

Controller listing window

Displays a list of available controllers.

OK

Click this button to add the reset use limit action for the selected controller(s) and exit out of the Reset Use Limit Properties window.

Note: Each time a use-limited badge is used at a reader, the badge's use limit is decremented for the associated controller. A cardholder's use limit is specified on the Badge form of the Cardholders folder. Whenever the cardholder swipes their badge at a reader where use limits are enforced, the cardholder's use limit is reduced by one (1). When the use count reaches zero (0), the cardholder is unable to access use limit-enforced card readers on that controller.

Cancel

Click this button to exit the Reset Use Limit Properties window without adding the action.

Help

Click this button to display online help for this window.

Reset Use Limit Properties Window Procedures

The following procedures can be performed on this form.

Add a Reset Use Limit Action

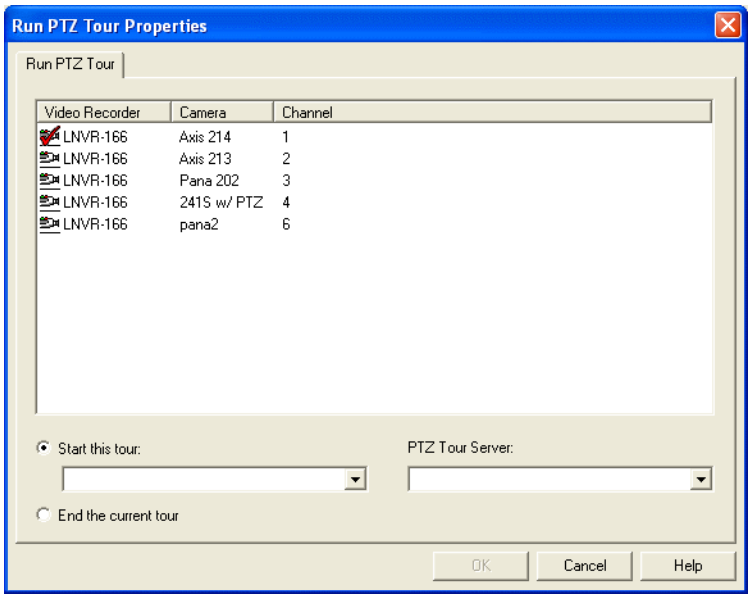
1. Open the Reset Use Limit Properties window using the Action Group Library, Scheduler, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) one or more controller from the listing window.
3. If you selected one controller from the listing window, skip this step. If you selected more than one controller from the listing window, type a descriptive name to identify the selected group of controllers in the **Description** field.
4. Click [OK].

Run PTZ Tour Properties Window

The Run PTZ Tour action type allows the user to start or end a continuous background PTZ tour. To use this action, a PTZ Tour Server must be configured in System Administration and a PTZ tour must be created in Alarm Monitoring.

Background PTZ tours can be interrupted by a user with a higher priority or by the user that started the tour. If a background PTZ tour is interrupted by the user that started it, the tour may fail to stop and control may not become available to the user. This issue will occur for any user of the same priority as the user who created the tour. In order for this not to occur, the user who creates the tour must have a priority lower than that of any user wishing to interrupt it.

You can open the Run PTZ Tour Action window using Scheduler or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Listing window

Displays all of the cameras assigned to an LNVR recorder. To display only PTZ cameras, add the following line to the **ACS.INI** file in the `[DigitalVideo]` section:
`TestForPTZOnStartUp=1`

Start this tour

To begin a tour, select the radio button and choose a tour from the drop-down list.

PTZ Tour Server

Select the PTZ tour server that should run this tour.

End the current tour

Select this radio button to stop a tour that is currently running on the selected camera.

Run PTZ Tour Properties Window Procedures

The following procedures can be performed on this form.

Add a Run PTZ Tour Action

1. Open the Run PTZ Tour Action window using the Scheduler or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) the camera from the listing window.
3. To start a tour:
   a. Select the **Start this tour** radio button and select the tour from the drop-down list.
   b. Select the server to run the tour from the **PTZ Tour Server** drop-down list.

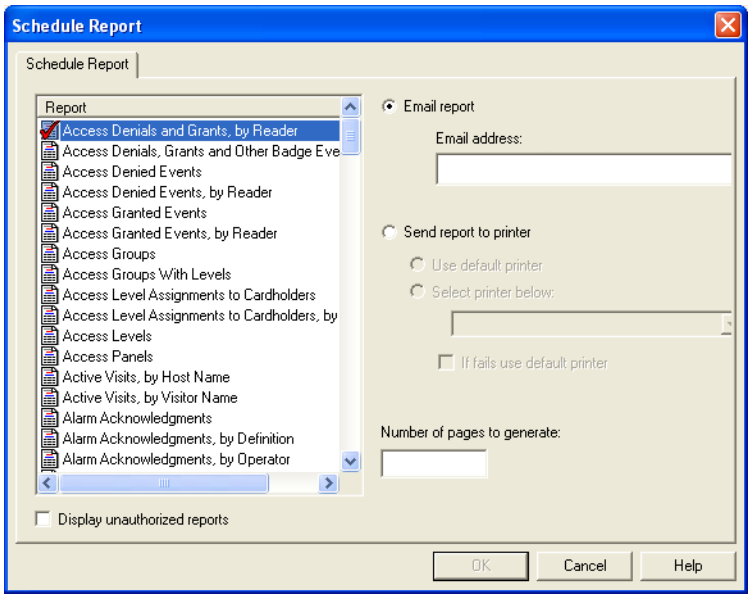
Note: Separate actions must be added to start and to end a PTZ tour. To end a tour, select the **End the current tour** radio button.

4. Click [OK].

Schedule Report Properties Window

The Schedule Report action type allows the user to either print a report or send a report in an email.

You can open the Schedule Report action window using Scheduler or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Report listing window

Displays a list of available reports.

Display unauthorized reports

By default, the schedule report only lists reports that users have permissions to preview. If the **Display unauthorized reports** check box is selected, reports that are disabled for a user will appear in the report listing window. The user can identify which reports are disabled by whether the [OK] button is inactive. This allows the user to ask the system administrator for permission to an existing report, if desired.

Reports are authorized and unauthorized by using report permission groups. For more information, refer to Report Permission Groups Form on page 371.

Email report

Select this radio button if you want the scheduled report to be sent in an email. E-mail notification requires the GOS module to be configured and running. For more information, refer to Chapter 26: Global Output Devices Folder on page 529.

Email address

Enter the email address where the scheduled report is to be sent.

Send Report to printer

Select this radio button if you want the scheduled report to print.

Use default printer

Select this radio button if you want the scheduled report to print from the workstation's default printer.

Select printer below

Select this radio button and choose a printer from the drop-down list if you want the scheduled report to print to a printer other than the workstation's default printer.

Note: The choices in the drop-down list are printers that are available for the computer running the linkage server and not for the workstation that the action is being configured on.

If fails use default printer

If you selected the **Select printer below** radio button, select this check box if you want to print from the default printer if the selected printer does not exist.

Note: Due to a limitation of Crystal Reports this setting is not enforced if the printer exists but is not accessible under the linkage server account. When this occurs the report will automatically be printed from the default printer regardless of this setting. For more information, refer to Request Print Action Flowchart on page 1254.

Number or pages to generate

When configuring a scheduled report action, you can enter the number of pages that you want the report to have. This can be helpful when only a small section of a large report is needed.

Schedule Report Properties Window Procedures

The following procedures can be performed on this form.

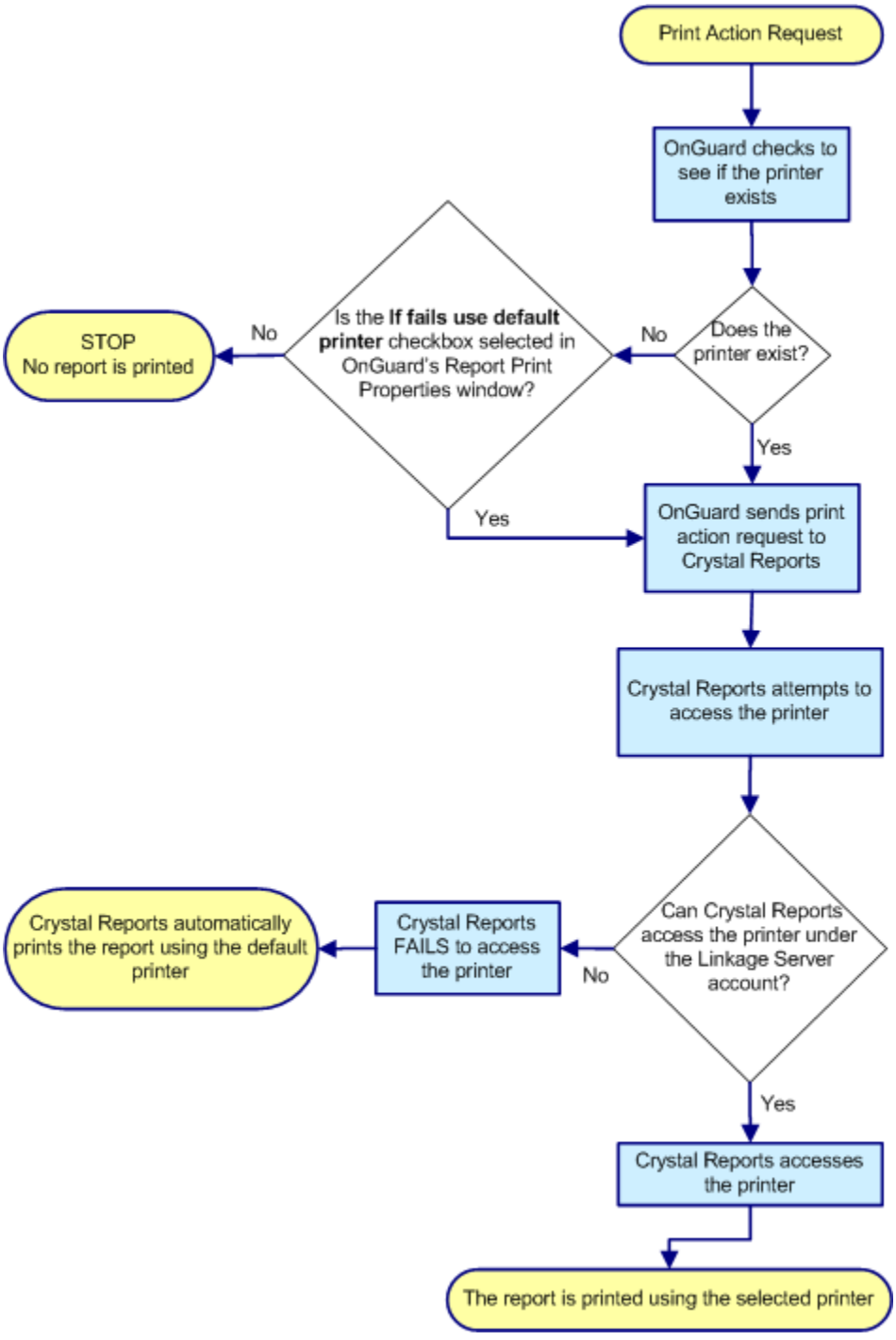
Add a Schedule Report Action

1. Open the Schedule Report Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select the report from the listing window.
3. Select whether the report is to be printed or sent in an email.
   - If the report is being sent in an email, select the **Email report** radio button and add an email address to the **Email Address** field.

     IMPORTANT: E-mail notification requires the GOS module to be configured and running. For more information, refer to the Global Output Devices Folder chapter in the System Administration User Guide.
   - If the report is being printed, select the **Send report to printer** radio button and select the printer to be used.
4. Select how many pages will be sent in an email or printed by entering a number in the **Number of pages to generate** field.
5. Click [OK].

   IMPORTANT: The Scheduled Report Action will not run unless the user who creates the action has an internal account. This is because the user account that creates the action is used to generate the report, and might not be configured for Single Sign-on at every workstation.

Request Print Action Flowchart



This flowchart shows how a report may get printed from the default printer although the **If fails use default printer** check box is NOT selected in the Report Print Properties window.

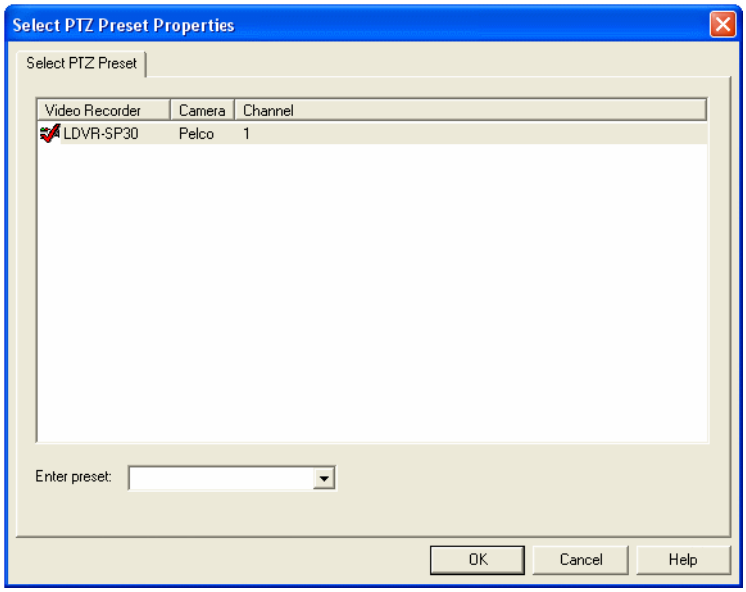
Select PTZ Preset Properties Window

The Select PTZ Preset action type allows users to select a preset for a PTZ camera to move to when the action is executed. This action is for camera and client side presets with network cameras assigned to an LNVR recorder.

Notes: The camera must be online when you configure the action.

The camera must be online when the action executes.

You can display the Select PTZ Preset Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Listing window

Displays all network cameras assigned to an LNVR recorder.

To display only PTZ cameras, add the following line to the **ACS.INI** file in the `[DigitalVideo]` section: `TestForPTZOnStartUp=1`

Note: The camera must be online when you configure the action and the camera must be online when the action executes.

Enter preset

Enter the camera side preset number or select a client side preset from the drop-down list.

Select PTZ Preset Properties Window Procedures

The following procedures can be performed on this form.

Add a Select PTZ Preset Action

1. Open the Select PTZ Preset Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Select (place a checkmark beside) the video recorder/camera/channel option from the listing window.

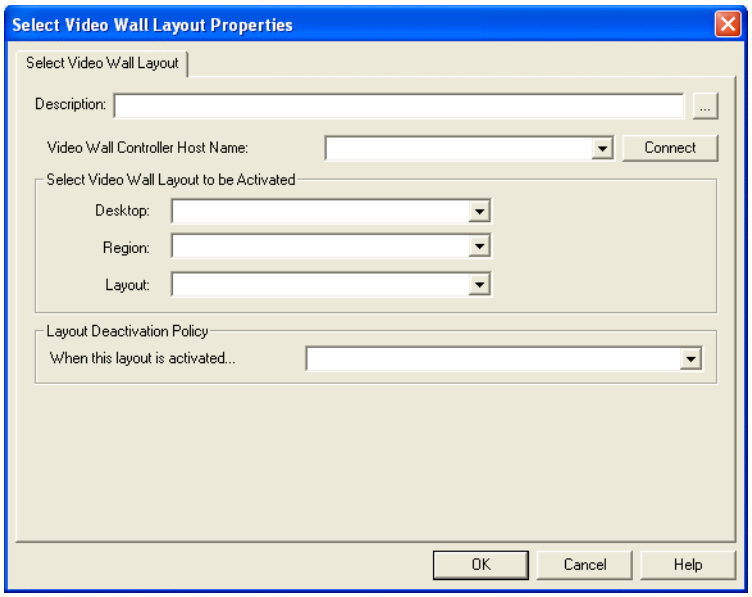
Note: The camera must be online when you configure the action and the camera must be online when the action executes.

3. Enter a camera side preset value or select a client side preset from the drop-down list.
4. Click [OK].

Select Video Wall Layout Properties Window

The Select Video Wall Layout action type allows users to activate and deactivate pre-configured layouts on the Barco video wall. Before this action is configured, video wall layouts must be defined using external software such as the Barco Apollo Explorer.

You can display the Select Video Wall Layout Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Description

A descriptive name for the action. After the Select Video Wall Layout to be Activate section of the dialog is configured, [...] can be used to automatically generate a name based on the controller, desktop, region, and layout names.

Video Wall Controller Host Name

Host name or IP address of the Barco Apollo server that controls the video wall. The drop-down list is populated by controller names that have been configured in other instances of the Select Video Wall Layout action.

Connect

Click to retrieve video wall layout information from the video wall controller to populate the drop-down lists in the Select Video Wall Layout to be Activated section.

Desktop

Identifies which physical video wall is being configured.

Region

If regions are enabled on the video wall, select one from the **Region** drop-down list.

Note: Regions are used to logically separate content so that multiple users can work in parallel without affecting each other.

Layout

Identifies the layout to be activated by the action. Layouts are configured in the Barco Apollo Explorer.

When this layout is activated...

Specifies the policy for deactivation of a layout that may be already active on the video wall.

- Deactivate All Layouts - Deactivates all layouts that are active on the video wall regardless of region.
- Deactivate Layouts in the Current Region - Deactivates layouts that are active in the region indicated in the **Region** drop-down list.
- Do Not Deactivate Any Layouts - Adds the new layout without deactivating any currently active layouts.

Select Video Wall Layout Properties Window Procedures

The following procedures can be performed on this form.

Add a Select Video Wall Layout Action

Before configuring this action, the video wall must be fully configured. For more information, refer to the Digital Video Hardware User Guide

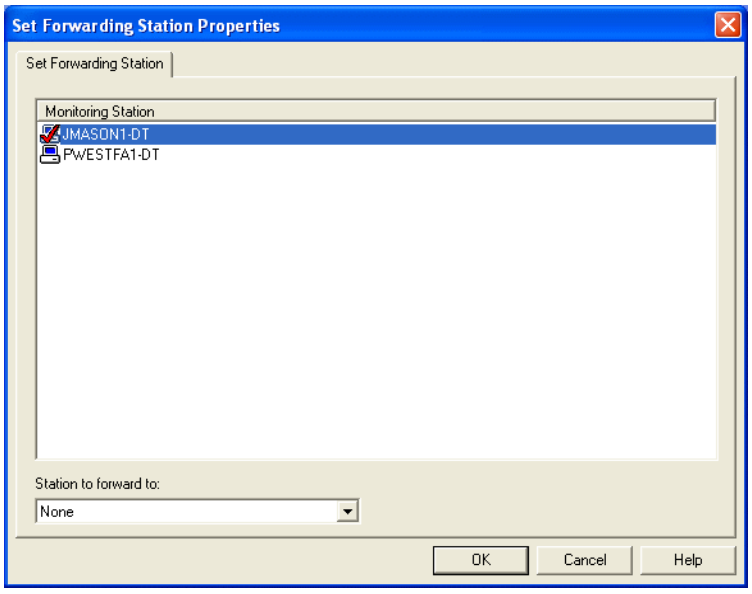
1. Open the Select Video Wall Layout Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Enter the host name or IP address of the Barco Apollo server that controls the video wall in the **Video Wall Controller Host Name** field or select a controller from the drop-down list.
3. Select the **Desktop** name from the drop-down list.
4. If your Barco configuration utilizes regions, select the appropriate one from the **Region** drop-down list.
5. Select the **Layout** to activate from the drop-down list.

6. Specify the Layout Deactivation Policy by selecting an action for currently active layouts from the **When this layout is activated...** drop-down list.
   - Deactivate All Layouts - Deactivates all layouts that are active on the video wall regardless of region.
   - Deactivate Layouts in the Current Region - Deactivates layouts that are active in the region indicated in the **Region** drop-down list.
   - Do Not Deactivate Any Layouts - Adds the new layout without deactivating any currently active layouts.
7. Enter a descriptive name for the action or use [...] to generate a name for the **Description** field based on the selected desktop, region, and layout names.
8. Click [OK] to save the action.

Set Forwarding Station Properties Window

The Set Forwarding Station action allows you to change where a monitor station forwards its alarms. Using this action allows a monitor station to be configured to forward its alarms to a different monitoring station.

Note: The action is only valid for a scheduler invocation.



Monitor Station listing window

Lists the monitoring stations available. Select the monitoring station that is having its alarms forwarded.

Station to forward to

Select the monitor station you would like the alarms forwarded to.

OK

Click this button to add the action and exit out of the Set Forwarding Station properties window.

Cancel

Click this button to exit the Set Forwarding Station properties window without adding the action.

Help

Click this button to display online help for this window.

Set Forwarding Station Properties Window Procedures

The following procedures can be performed on this form.

Add a Set Forwarding Station Action

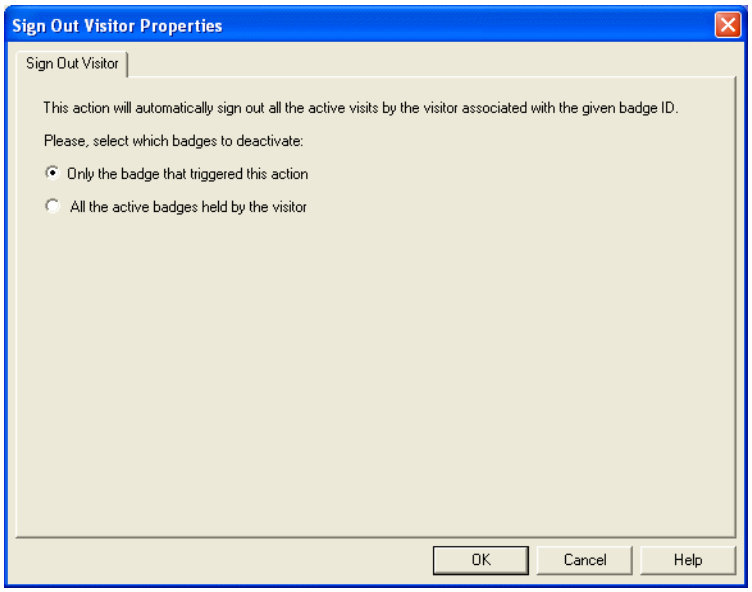
1. Open the Set Forwarding Station Properties window, using Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Choose the monitor station in the Monitoring Station list window. This will be the monitor station that has its alarms forwarded to another monitoring station.
3. In the **Station to forward to** drop-down box, choose the monitoring station that the alarms will be forwarded to.
4. Click [OK].

Sign Out Visitor Properties Window

The Sign Out Visitor action allows you to deactivate the badges of cardholders who have signed out of the system. You can further modify this action by choosing which of the cardholder's badges will be signed out, just the badge that triggered the action or all badges belonging to that cardholder.

You can display the Sign Out Visitor Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 1194.

Note: In segmented systems, the Sign Out Visitor Properties action must be applied to all segments.



Only the badge that triggered this action
Select if you want to deactivate only the badge that caused the visitor to sign out.

All the active badges held by the visitor
Select if you want all the badges belonging to the visitor to deactivate once the visitor is signed out.

OK
Click this button to add the action and exit out of the Sign Out Visitor properties window.

Cancel
Click this button to exit the Sign Out Visitor properties window without adding the action.

Help
Click this button to display online help for this window.

Sign Out Visitor Properties Window Procedures

The following procedures can be performed on this form.

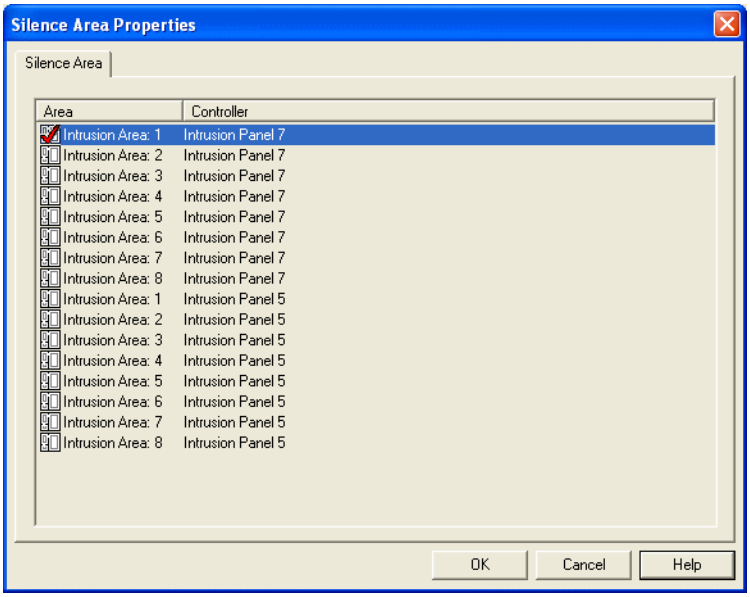
Add a Sign Out Visitor Action

1. Open the Sign Out Visitor Properties window, using Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. Choose the options that suit your needs.
3. Click [OK].

Silence Area Properties Window

The Silence Area action allows an area (that uses a Bosch intrusion panel) to be silenced during an alarm from that panel.

You can display the Silence Area Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Listing window

Lists currently enabled intrusion areas. Intrusion areas are configured on the Areas form in the Intrusion Detection Configuration folder. For more information, refer to Areas Form on page 1140.

OK

Click this button to add the action and exit out of the Silence Area Properties window.

Cancel

Click this button to exit the Silence Area Properties window without adding the action.

Help

Click this button to display online help for this window.

Silence Area Properties Window Procedures

The following procedures can be performed on this form.

Add a Silence Area Action

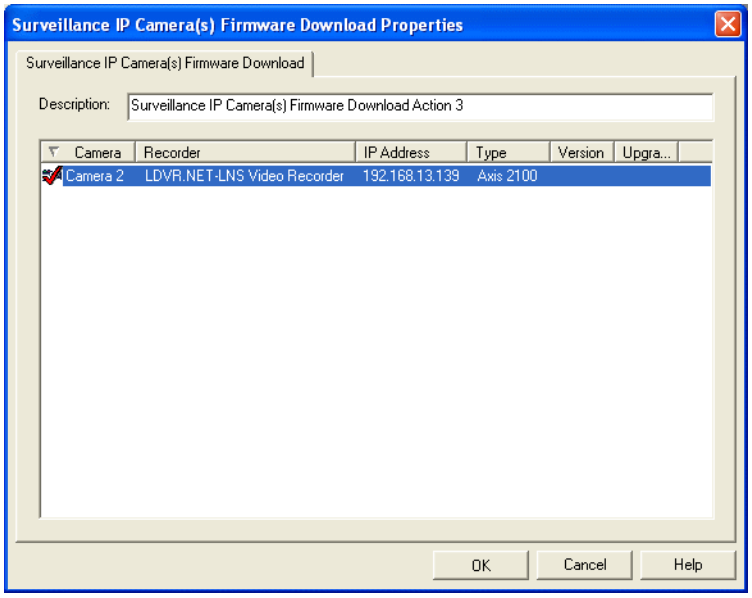
1. Open the Silence Area Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 1194.
2. From the listing window, click on an entry to select it. The area you selected will now be silenced during an alarm from that panel.

   IMPORTANT: The silence area action can only be used with Bosch intrusion panels.
3. Click [OK].

Surveillance IP Camera(s) Firmware Download Properties Window

The Surveillance IP Camera(s) Firmware Download action is for upgrading the firmware on surveillance only cameras in which no LNVR is used.

You can display the Surveillance IP Camera(s) Firmware Download Properties window using the Action Group Library or Scheduler.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 24: Scheduler Folder on page 515.

Description

Displays a descriptive name for this action. A default name is automatically entered in this field, however, in modify mode you can enter any name you choose.

Camera listing window

Displays the names of the IP cameras that are available for selection.

OK
Click this button to add the action and exit out of the Surveillance IP Camera(s) Firmware Properties window.

Cancel
Click this button to exit the Surveillance IP Camera(s) Firmware Properties window without adding the action.

Help
Click this button to display online help for this window.

Surveillance IP Camera (s) Firmware Download Properties Window Procedures

The following procedures can be performed on this form.

Add a Surveillance IP Camera(s) Firmware Download Action

1. Open the Surveillance IP Camera(s) Firmware Download Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 1194.
2. In the **Description** field, enter a descriptive name for this action. If you would like to use the default name (which is automatically entered when you display the Surveillance IP Camera(s) Firmware Download Properties window), you can skip this step.
3. From the Camera listing window, select an IP camera.
4. Click [OK].

APPENDIX B

Alarm/Event Descriptions

Alarm	Event	Event Type	Description	Duress*
24 Hour Alarm	24 Hour Alarm	Trouble	A 24 hour alarm condition has been detected.	
24 Hour Alarm Restore	24 Hour Alarm Restore	Trouble	A 24 hour alarm condition has been restored.	
24 Hour Auto Test	24 Hour Auto Test	Trouble		
24 Hour Non-Burglary Alarm	24 Hour Non-Burglary Alarm	Trouble	A 24 hour non-burglary alarm condition has been detected.	
24 Hour Report Closed	24 Hour Report Closed	Trouble	A 24 Hour report on a closed zone	
24 Hour Report Open	24 Hour Report Open	Trouble	A 24 Hour report on an open zone	
24 Hour Zone Bypassed	24 Hour Zone Bypassed	Trouble	A 24 hour zone has been bypassed.	
24 Hour Zone Unbypassed	24 Hour Zone Unbypassed	Trouble	A 24 hour zone has been unbypassed.	
30 Minutes Since Fallback Command	30 Minutes Since Fallback Command	Trouble	30 minutes have passed since fallback command.	
32 Hour Event Log Marker	32 Hour Event Log Marker	System		
Abort	Abort	System	An event message was not sent due to User action	

Alarm	Event	Event Type	Description	Duress*
AC Restore	AC Restore	System	AC power trouble has been restored.	
AC Trouble	AC Trouble	System	An AC power trouble condition has been detected.	
Accepted Biometric Score	Accepted Biometric Score	Biometric	This event returns the accepted biometric score. The actual access granted event is sent separately. This event is mainly used for diagnostic purposes.	
Access Closed	Access Closed	Denied	Access for all users prohibited.	
Access Code Used	Access Code Used	Denied	Access code was used.	
Access Denied	Access Denied	Denied	Access was denied.	
Access Denied to Destination Floor	Access Denied to Destination Floor	Denied	Generated when a card was presented to a reader associated with an elevator terminal but the elevator assignment was not performed; used when elevator dispatching devices are present.	
Access Denied: Access Control Format Not Found	Access Denied: Access Control Format Not Found	Denied	Generated when there are no ACFs (Access Control Formats) stored at the lock.	
Access Denied: Area Empty	Access Denied	Denied	An event indicating that access was denied due to the room being empty.	Yes
Access Denied: Area Occupied	Access Denied	Denied	An event indicating that access was denied due to the room being empty.	Yes
Access Denied: Asset Required	Access Denied	Denied	An event indicating that access was denied since no asset was presented for the access attempt.	Yes
Access Denied: Biometric Reader Offline	Access Denied: Biometric Reader Offline	Denied	Generated when the alternate biometric reader could not be contacted for verification (was offline).	Yes

Alarm	Event	Event Type	Description	Duress*
Access Denied: Card Expired	Access Denied: Card Expired	Denied	Card has expired.	
Access Denied: Escort Timeout Expired	Access Denied: Escort Timeout Expired	Denied	This event indicates that access was denied because a person requiring an escort attempted access but an escort did not present their credentials in the time period.	Yes
Access Denied: Door Secured	Access Denied: Door Secured	Denied	Access denied because door was secured.	
Access Denied: Interlock	Access Denied: Interlock	Denied	An access request was denied because the doors associated Interlock point is open.	
Access Denied: Invalid Access Control Data	Access Denied: Invalid Access Control Data	Denied	Failed to process Integra card data.	
Access Denied: Invalid Access Control Data Length	Access Denied: Invalid Access Control Data Length	Denied	The length of the retrieved data did not match the length specified in selected ACF (Access Control Format).	
Access Denied: Invalid Access Control Data Parity	Access Denied: Invalid Access Control Data Parity	Denied	Parity calculations for retrieved data failed for selected ACF (Access Control Format).	
Access Denied: Invalid Access Control Data Type	Access Denied: Invalid Access Control Data Type	Denied	The type of retrieved data (Wiegand/Integra) did not match the ACF (Access Control Format) type.	
Access Denied: Invalid Smart Card Authentication	Access Denied: Invalid Smart Card Authentication	Denied	Failed to authenticate to the application specified by the selected SCF (Smart Card Format).	
Access Denied: Invalid Smart Card Data	Access Denied: Invalid Smart Card Data	Denied	Failed to retrieve HID application data; invalid header, invalid data length.	
Access Denied: Invalid Smart Card Location	Access Denied: Invalid Smart Card Location	Denied	Application data could not be located on the card based on the selected SCF (Smart Card Format).	

Alarm	Event	Event Type	Description	Duress*
Access Denied: Invalid Smart Card Type	Access Denied: Invalid Smart Card Type	Denied	Either the card was not found in the field or the card failed to respond to the requested RF (Radio Frequency) protocol.	
Access Denied: No Biometric Template	Access Denied: No Biometric Template	Denied	Generated when the cardholder did not have a biometric template loaded in the database, so a verification could not be done.	Yes
Access Denied: No Occupant Approval	Access Denied: No Occupant Approval	Denied	An event indicating that access was denied due to no occupant approval.	Yes
Access Denied: Passback	Access Denied: Passback	Denied	Access was denied because the credential has not exited the area before attempting to re-enter same area.	
Access Denied: Reader Locked	Access Denied: Reader Locked	Denied	Generated when access was denied because the reader was locked.	Yes
Access Denied: Secured Mode	Access Denied: Secured Mode	Denied	Lock is in secured mode; no users will be allowed access.	
Access Denied: Smart Card Format Not Found	Access Denied: Smart Card Format Not Found	Denied	No SCFs (Smart Card Formats) stored at the lock.	
Access Denied: Unauthorized Arming State	Access Denied: Unauthorized Arming State	Denied	An access request was denied because the user was not authorized in this area when the area was armed.	
Access Denied: Unauthorized Entry Level	Access Denied: Unauthorized Entry Level	Denied	An access request was denied because the user is not authorized in this area.	
Access Denied: Unauthorized Time	Access Denied: Unauthorized Time	Denied	An access request was denied because the request is occurring outside the user's authorized time window(s).	
Access Door Propped	Access Door Propped	System		

Alarm	Event	Event Type	Description	Duress*
Access Door Status Monitor Shunt	Access Door Status Monitor Shunt	System		
Access Door Status Monitor Trouble	Access Door Status Monitor Trouble	System		
Access Granted	Access Granted	Granted	Access was granted.	Yes
Access Granted	Granted Access	Granted	Access was granted.	
Access Granted to Destination Floor	Access Granted to Destination Floor	Granted	Generated when a card was presented to a reader associated with an elevator terminal and the elevator cab assignment was performed; used when elevator dispatching devices are present.	
Access Granted - Anti-Passback Not Used	Granted APB Violation, No Entry Made	Area APB	Indicates that an anti-passback violation resulted and access was granted but no entry was made. This can happen when using soft anti-passback.	Yes
Access Granted - Anti-Passback Used	Granted APB Violation, Entry Made	Area APB	Indicates that an anti-passback violation resulted but access was granted and entry was made. This can happen when using soft anti-passback.	Yes
Access Granted - Entry Made	Access Granted - Entry Made	Granted	Access granted and door opened; used when latch or door sensor monitoring is present.	
Access Granted - No Entry Made	Granted No Entry	Granted	Access was granted but door not opened; used when latch or door sensor monitoring is present.	
Access Granted on Facility Code	Granted Facility Code	Granted	Access was granted based on a valid facility code.	Yes
Access Granted on Facility Code, No Entry Made	Granted Facility Code, No Entry	Granted	Access was granted on facility code but no entry was made at the door.	Yes

Alarm	Event	Event Type	Description	Duress*
Access Granted: Reader Unlocked	Access Granted: Reader Unlocked	Granted	Generated when access was granted because the reader was unlocked.	Yes
Access Granted Under Duress	Access Granted Under Duress	Duress	Indicates that the cardholder was granted access under duress.	Yes
Access Granted Under Duress - No Entry Made	Access Granted Under Duress - No Entry Made	Duress	Access Granted Under Duress - No Entry Made	Yes
Access Level Change	Access Level Change	System		
Access Lockout	Access Lockout	System	Access denied, known code	
Access Open	Access Open	System	Access for authorized users in now allowed	
Access Point Bypass	Access Point Bypass	System		
Access Program Exit	Access Program Exit	System		
Access Relay/ Trigger Fail	Access Relay/ Trigger Fail	System		
Access Request to Exit Shunt	Access Request to Exit Shunt	System		
Access Schedule Change	Access Schedule Change	System	The access schedule has changed.	
Access Trouble	Access Trouble	System	An access system trouble condition has been detected.	
Access Zone Shunt	Access Zone Shunt	System	An access zone is put in the shunted state.	
Account Status Failure	Account Status Failure	System		
Account Status Restore	Account Status Restore	System		
Acknowledgment Action Executed	Acknowledgment Action Executed	System	Generated when an alarm is acknowledged and actions associated with the alarm are executed.	

Alarm	Event	Event Type	Description	Duress*
Acknowledgment Action Failed	Acknowledgment Action Failed	System	Generated when there is a failure to execute actions associated with an alarm acknowledgment.	
Activate Output	Activate Output	System		
Activity Resumed	Activity Resumed	System	A zone has detected activity after an alert.	
ACU Firmware Upgraded	ACU Firmware Upgraded	System	Lock firmware was updated.	
Air Flow Loss	Air Flow Loss	Trouble	An air flow loss condition has been detected.	
Air Flow Loss Restore	Air Flow Loss Restore	Trouble	An air flow loss condition has been restored.	
Alarm	Alarm	System		
Alarm Active	Alarm Active	System	Generated when an alarm has become active.	
Alarm Canceled	Alarm Restored	System	A device has come online or an alarm condition has been restored.	
Alarm Mask Group Armed			This event is generated when the alarm mask group is armed.	
Alarm Mask Group Disarmed			This event is generated when the alarm mask group is disarmed.	
Alarm Mask Group Force Armed			This event is generated when the alarm mask group is force armed.	
Alarm Mask Group Mask Count Incremented			This event is generated when a disarm command is issued and the alarm mask group is already disarmed, causing the alarm mask count to get incremented. The alarm mask group will still remain disarmed.	

Alarm	Event	Event Type	Description	Duress*
Alarm Mask Group Mask Count Decremented			This event is generated when an arm or force arm command is issued and the alarm mask group has a mask count greater than 1, causing the mask count to be decremented. The alarm mask group will still remain disarmed.	
Alarm Mask Group Arming Failure, Active Points			The following command is used to indicate an arming failure due to active points. This command should be hard to generate because currently the only way to issue the standard arm command is from the command keypad and this should only be available if there are no active points.	
Alarm Monitoring Action Group Executed	Alarm Monitoring Action Group Executed	System	Generated when the action group is executed.	
Alarm Monitoring Action Group Failed	Alarm Monitoring Action Group Failed	System	Generated when the action group execution fails.	
Alarm Relay Disable	Alarm Relay Disable	System		
Alarm Relay Disable Restored	Alarm Relay Disable Restored	System		
Alarm/Restore	Alarm/Restore	System	Generated when a device has come online or an alarm condition has been restored.	
Alarm Silenced	Alarm Silenced	System		
Alarm Tamper Loop	Alarm Tamper Loop	Trouble		
All Points Tested	All Points Tested	System	All points have been tested.	

Alarm	Event	Event Type	Description	Duress*
All Systems Normal	All Systems Normal	Fire	Generated when the Notifier AM-2020 panel is booted up. This alarm may also be sent when all existing alarm conditions are resolved.	
Analog Restore	Analog Restore	Fire		
Analog Restored	Analog Restored	System		
Analog Service Requested	Analog Service Requested	System		
Analog Service Required	Analog Service Required	Fire	An analog fire sensor needs to be cleaned or calibrated.	
Anti-Passback Violation	Anti-Passback Violation	Area Control	Generated when the cardholder was denied access because the entry would have violated the anti-passback rules for the area.	Yes
Archive Server Failure	Archive Server Failure	Video	Generic error indicating a failure on the archive server. This error indicates that the archive server could not move any more data from the video recorders to the archive server. The user will have to go to the physical archive server computer and review the remote storage application and logs, OnGuard log files in the OnGuard\logs directory, and also follow general trouble shooting techniques as outlined in the archive server manual to determine the specific cause of the alarm.	

Alarm	Event	Event Type	Description	Duress*
Archive Server Failure Archive Location Full	Archive Server Failure	Video	This error indicates that the archive location is full and no further data can be moved from the video recorders to the archive server. If this issue is not resolved, it is possible events may be purged before they are archived.	
ARDIS Module Communication Loss	ARDIS Module Communication Loss	Trouble		
ARDIS Module Communication Restored	ARDIS Module Communication Restored	Trouble		
Area Closed	Area Closed	Area Control	Generated when access was denied because the area being entered is closed.	Yes
Area Limit Exceeded	Area Limit Exceeded	Area Control	Generated when access was denied because the area limit would have been exceeded.	Yes
Area Watch End	Area Watch End	System	Area watch feature has been deactivated	
Area Watch Start	Area Watch Start	System	Area watch feature has been activated	
Arm/Disarm Command Accepted			This event will be generated when the arm/ disarm command is issued at a reader. It will also report back an additional event parameter indicating “No Action”, “Disarmed”, “Armed”, “Forced Armed”	

Alarm	Event	Event Type	Description	Duress*
Arm/Disarm Command Denied			This event will be generated when the arm/ disarm command is attempted at a reader but is denied. It will also report back an additional event parameter indicating the reason for failure: “No Command Authority”, “Not Allowed at Reader”, “Invalid Arguments”.	
Armed Perimeter Delay	Armed Perimeter Delay	System		
Armed Perimeter Instant	Armed Perimeter Instant	System		
Armed Stay	Armed Stay	System		
Asset Denied - Invalid Access	Asset Denied - Invalid Access	Asset	Generated when the asset was denied because the cardholder had invalid access levels.	Yes
Asset Denied - Invalid Asset	Asset Denied - Invalid Asset	Asset	Generated when the asset was denied because of an invalid asset (the asset was not found in the controller).	Yes
Asset Denied - Invalid Cardholder	Asset Denied - Invalid Cardholder	Asset	Generated when the asset was denied because of an invalid cardholder.	Yes
Asset Denied - No Asset Privileges	Asset Denied - No Asset Privileges	Asset	Generated when the asset was denied because the cardholder had no asset privileges.	
Asset Granted - Asset Owner	Asset Granted - Asset Owner	Asset	Generated when the asset was granted because the cardholder was the asset owner.	Yes
Asset Granted - Asset Privileges Only	Asset Granted - Asset Privileges Only	Asset	Generated when the asset was granted because the cardholder had asset privileges.	Yes
Audible Alarm	Audible Alarm	Trouble	An audible alarm condition has been detected.	

Alarm	Event	Event Type	Description	Duress*
Audible Alarm Restore	Audible Alarm Restore	Trouble	An audible alarm condition has been restored.	
Audibles Silenced	Audibles Silenced	Fire	Generated when all the alarm bells have been turned off on the controller.	
Audibles Unsilenced	Audibles Unsilenced	Fire	Generated when all the alarm bells have been turned back on for the controller.	
Audit Trail Cleared	Audit Trail Cleared	System	Generated when the audit (event) log is cleared.	
Audit Trail Limit Reached	Audit Trail Limit Reached	System	Informs OnGuard the audit (event) log is becoming full and will be overwritten.	
Auto Arming Time Changed	Auto Arming Time Changed	System		
Auto-Arm Failed	Auto-Arm Failed	Trouble	An automatic arm has failed.	
Automatic Closing	Automatic Closing	Open/ Close	The system was armed automatically.	
Automatic Opening	Automatic Opening	Open/ Close	The system has disarmed automatically.	
Automatic Phone Test	Automatic Phone Test	System		
Automatic Test	Automatic Test	System	Automatic communication test report	
Auxiliary Power Fault	Auxiliary Power Fault	Trouble		
Auxiliary Power Supply AC Loss	Auxiliary Power Supply AC Loss	Trouble		
Auxiliary Power Supply AC Restored	Auxiliary Power Supply AC Restored	Trouble		
Auxiliary Power Supply Communication Loss	Auxiliary Power Supply Communication Loss	Trouble		

Alarm	Event	Event Type	Description	Duress*
Auxiliary Power Supply Communication Restored	Auxiliary Power Supply Communication Restored	Trouble		
Auxiliary Power Supply Communication Restored	Auxiliary Power Supply Communication Restored	Trouble		
Auxiliary Power Supply Fault Restored	Auxiliary Power Supply Fault Restored	Trouble		
Auxiliary Power Supply Output Low	Auxiliary Power Supply Output Low	Trouble		
Auxiliary Power Supply Output Low Restored	Auxiliary Power Supply Output Low Restored	Trouble		
Background Map Found	Background Map Found	Video	Generated when background stickers are detected.	
Background Map Not Found	Background Map Not Found	Video	Generated when the engine cannot detect the background stickers. This may be caused when there is poor contrast or the stickers are improperly shaped/ separated.	
Background Scene Changed	Background Scene Changed	Video	Indicates that part of the background has changed. This can be from something added to the scene or something removed from the scene.	
Background Scene Change Restored	Background Scene Change Restored	Video	The alarm is restored.	
Bad 9112 Packet	Bad 9112 Packet	System		
Battery Test Fail	Battery Test Fail	System	A battery test fail condition has been detected.	

Alarm	Event	Event Type	Description	Duress*
Battery Test Fail Restore	Battery Test Fail Restore	System	A battery test fail condition has been restored.	
Bell # Disable	Bell # Disable	Relay/ Sounder	Bell # has been disabled.	
Bell # Disable Restore	Bell # Disable Restore	Relay/ Sounder	Bell # has been restored.	
Bell Fault	Bell Fault	Relay/ Sounder	A trouble condition has been detected on a local bell, siren, or annunciator.	
Bell Restore	Bell Restore	Relay/ Sounder	A trouble condition has been restored on a local bell, siren, or annunciator.	
Biometric Mismatch	Biometric Mismatch	Denied	Generated when the cardholder has a biometric template and the alternate reader was utilized to capture a template to match, but the captured template did not match the stored template.	Yes
Biometric Verify Mode Disabled	Biometric Verify Mode Disabled	System	Generated when biometric verify mode is disabled.	
Biometric Verify Mode Enabled	Biometric Verify Mode Enabled	System	Generated when biometric verify mode is enabled.	
Blind Camera (AI)	Blind Camera (AI)	Video	Indicates that level of camera blindness (covered by some sort of obstacle) exceeded configured threshold.	
Blind Camera (AI) Restored	Blind Camera (AI) Restored	Video	The alarm is restored.	
Block Acknowledge	Block Acknowledge	Fire	Generated when a block acknowledge command is sent. This command acknowledges any existing unacknowledged alarms in the system all at once.	

Alarm	Event	Event Type	Description	Duress*
Brightness Change	Brightness Change	Video	Generated when a change in overall brightness level of the scene is detected.	
Brightness Change Restored	Brightness Change Restored	Video	Generated when changes in brightness level are no longer exceeding the user defined threshold.	
Burglary Alarm	Burglary Alarm	Burglary	A burglary alarm condition has been detected.	
Burglary Alarm Cross Point	Burglary Alarm Cross Point	Burglary		
Burglary Alarm Restore	Burglary Alarm Restore	Burglary	A burglary alarm condition has been restored.	
Burglary Bypass	Burglary Bypass	Burglary	A burglary zone has been bypassed.	
Burglary Cancel	Burglary Cancel	Burglary	A burglary zone has been cancelled by an authorized user.	
Burglary Close	Burglary Close	Open/ Close		
Burglary Inactive	Burglary Inactive	Burglary		
Burglary Open	Burglary Open	Open/ Close		
Burglary Restore	Burglary Restore	Burglary	A burglary alarm/trouble condition has been eliminated.	
Burglary Supervisory	Burglary Supervisory	Burglary	An unsafe intrusion detection system condition has been detected.	
Burglary Test	Burglary Test	Burglary	A burglary zone has been activated during testing.	
Burglary Trouble	Burglary Trouble	Burglary	A burglary trouble condition has been detected.	
Burglary Trouble Restore	Burglary Trouble Restore	Burglary	A burglary trouble condition has been restored.	

Alarm	Event	Event Type	Description	Duress*
Burglary Unbypass	Burglary Unbypass	Burglary	Burglary zone bypass has been removed.	
Burglary Verified	Burglary Verified	Burglary	A burglary alarm has occurred and been verified within programmed conditions.	
Busy Seconds	Busy Seconds	System	The percent of time the receiver's line card is online.	
Bypass - Closed	Bypass - Closed	Open/ Close		
Bypass Restore	Bypass Restore	System		
C900 Battery Low	C900 Battery Low	C900		
C900 Battery Restore	C900 Battery Restore	C900		
C900 Input Open	C900 Input Open	C900		
C900 Input Restored	C900 Input Restored	C900		
C900 Input Shorted	C900 Input Shorted	C900		
C900 Intercepted Disabled	C900 Intercepted Disabled	C900		
C900 Intercepted Enabled	C900 Intercepted Enabled	C900		
C900 Output Activated	C900 Output Activated	C900		
C900 Output Deactivated	C900 Output Deactivated	C900		
C900 Reboot	C900 Reboot	C900		
C900 Switched to Fallback	C900 Switched to Fallback	C900		
C900 Switched to Intercept	C900 Switched to Intercept	C900		
Cabinet Tamper Active	Cabinet Tamper	System	Generated when a cabinet tamper condition has been detected.	
Cabinet Tamper Restored	Cancelled Cabinet Tamper	System	Generated when a cabinet tamper condition has been restored.	
Callback Request	Callback Request	System		

Alarm	Event	Event Type	Description	Duress*
Callback Request	Call Conferenced	Intercom		
Call Disconnected	Call Disconnected	Intercom	Generated when an intercom call has been disconnected.	
Call Ended	Call Ended	Intercom	Generated when a call has ended.	
Call Established	Call Established	Intercom	Generated when an intercom call is answered.	
Call Failed	Call Failed	Intercom	Generated when an intercom call fails.	
Call to a busy subscriber	Call to a busy subscriber	Intercom	Generated when an intercom call has been placed to a busy subscriber.	
Call to an open subscriber	Call to an open subscriber	Intercom	Generated when an intercom call has been placed to an open subscriber.	
Call to a private subscriber	Call to a private subscriber	Intercom	Generated when a call has been placed to a private subscriber.	
Call Transferred	Call Transferred	Intercom	Generated when a call was transferred.	
Camera Enabled	Camera Enabled	NetDVMS	The camera is enabled in the NetDVMS Administrator.	
Camera Disabled	Camera Disabled	NetDVMS	The camera is disabled in the NetDVMS Administrator.	
Camera Motion	Camera Motion	NetDVMS	Generated when motion has been detected on a given input channel (camera). Motion is considered any change in the environment within the field of view of the camera. Sensitivity is determined by the motion detection settings in the NetDVMS Administrator.	

Alarm	Event	Event Type	Description	Duress*
Camera Tamper Active	Camera Tamper Active	Video	Indicates that IP Camera configuration was changed bypassing the OnGuard software. (It is possible if the user knows password to access the IP Camera and connect to it directly using IP Camera provided Web-interface.)	
Camera Tamper Restored	Camera Tamper Restored	Video	The alarm is restored. LNVR changed camera settings back to normal.	
Cancel Alarm	Cancel Alarm	System		
Cancel Entire Sale	Cancel Entire Sale	POS	Generated when a transaction is used to indicate that an entire sale was cancelled.	
Cancel Report	Cancel Report	System	Untyped zone cancel.	
Cannot Open Door: Interlock Area Busy	Cannot Open Door: Interlock Area Busy	Area Control	An attempt to open the door in Alarm Monitoring was denied because a door is open or the door strike is active within an interlocked area.	
Capture Source Mismatch	Capture Source Mismatch	Video	Indicates that user-specified IP Camera type in OnGuard does not match actual IP Camera type.	
Carbon Monoxide Detected	Carbon Monoxide Detected	Gas	Generated when carbon monoxide has been detected by an alarm.	
Card Added	Card Added	System	Generated when a card has been added.	
Card Assigned	Card Assigned	System	An access ID has been added to the controller.	
Card Deleted	Card Deleted	System	An access ID has been deleted from the controller.	
Card Only Mode Denied: Blocked Mode	Card Only Mode Denied: Blocked Mode	System	Automatic scheduled change to card only mode was denied because lock is in blocked mode.	

Alarm	Event	Event Type	Description	Duress*
Card Only Mode Denied: Secured Mode	Card Only Mode Denied: Secured Mode	System	Automatic scheduled change to card only mode was denied because lock is in secured mode.	
Cash Amount Tendered	Cash Amount Tendered	POS	Generated when an event is used to indicate that a cash amount has been tendered	
Cash or Safe Drop	Cash or Safe Drop	POS	Generated when a transaction indicating a cash or safe drop has occurred.	
Change Due	Change Due	POS	Generated when a transaction indicating the change due has occurred.	
Change of State	Change of State	System	An expansion/peripheral device is reporting a new condition or state change.	
Charge Account Tender	Charge Account Tender	POS	Generated when a charge account was used as tender.	
Check Tender	Check Tender	POS	Generated when a check was used as tender.	
Checksum Fail	Checksum Fail	System	A checksum failure has been detected.	
Cipher Mode Disabled	Cipher Mode Disabled	System	Generated when Cipher mode is disabled for a reader.	
Cipher Mode Enabled	Cipher Mode Enabled	System	Generated when cipher mode is enabled for a reader. When this occurs card data can be entered via the keypad.	
Clerk Name or Number	Clerk Name or Number	POS	A transaction that reports the clerk's name or number.	
Close Area	Close Area	Open/ Close	The system has been partially armed	
Close by User	Close by User	Open/ Close	The area has been armed by a user.	

Alarm	Event	Event Type	Description	Duress*
Close Exception	Close Exception	Open/ Close		
Close Out of Window	Close Out of Window	Open/ Close		
Closing	Closing	Open/ Close		
Closing Delinquent	Closing Delinquent	Open/ Close		
Closing Extend	Closing Extend	Open/ Close	The closing time has been extended.	
Closing Out of Window by User	Closing Out of Window by User	Open/ Close		
Closing Report	Closing Report	Open/ Close	The system is armed and normal	
Closing Switch	Closing Switch	Open/ Close		
Closing Time Changed	Closing Time Changed	Open/ Close		
Combustion Alarm	Combustion Alarm	Open/ Close	A combustion alarm condition has been detected.	
Combustion Alarm Restore	Combustion Alarm Restore	Open/ Close	A combustion alarm condition has been restored.	
Command (#) Set From Reader	Command (#) Set From Reader	System	Generated when the reader keypad command “(#)” was executed.	
Command Pin +10 Set From Reader	Command Pin +10 Set From Reader	System	Indicates the reader command “Pin +10” was executed.	
Command Pin +20 Set From Reader	Command Pin +20 Set From Reader	System	Indicates the reader command “Pin +20” was executed.	
Command Sent	Command Sent	System	A command has been sent to an expansion/ peripheral device.	
Communication Access Denied	Communication Access Denied	System	Indicates that a wrong password has been entered while logging on to a communication device.	

Alarm	Event	Event Type	Description	Duress*
Communication Initialization Failed	Communication Initialization Failed	System	Generated when the Communication Server fails to initialize communications. For example if you are using RS-232 and have hyperterminal running and using COM1 and then you start up the Communication Server and it needs to use COM1 to communicate to a panel, it will fail to open up the serial port and this event will be logged.	
Communication Trouble Restore	Communication Trouble Restore	System	A communication trouble has been restored.	
Communications Fail	Communications Fail	System	A communication has failed.	
Communications Lost	Communications Lost	System	Generated when communications to the device have been lost.	
Communications Lost - Primary Path	Primary Communication Path Lost	System	Generated when the primary path lost communication with the host.	
Communications Lost - Secondary Path	Secondary Communication Path Lost	System	Generated when the secondary path loses communication with the host.	
Communications Path Switched - Primary to Secondary	Communications Path Switched - Primary to Secondary	System	Generated when the communication path has been switched from the primary path to the secondary path.	
Communications Path Switched Secondary to Primary	Communications Path Switched Secondary to Primary	System	Generated when the communication path has switched from the secondary path to the primary path.	
Communications Restore	Communications Restore	System	Generated when communications have been restored.	
Communications Restored	Communications Restored	System	Generated when communications to the device have been restored.	

Alarm	Event	Event Type	Description	Duress*
Communications Restored - Primary Path	Primary Communication Path Restored	System	Generated when the primary path restored communication with the host.	
Communications Restored - Secondary Path	Secondary Communication Path Restored	System	Generated when the secondary path restored communication with the host.	
Communications Trouble	Communications Trouble	System	A communications trouble has been detected.	
Communications With Host Lost	Communications With Host Lost	System	An event was generated by the hardware when communications with the host was lost.	
Communications With Host Restored	Communications With Host Restored	System	An event was generated by the hardware when communications with the host was restored.	
Complimentary Tender	Complimentary Tender	POS	Generated when the tender was complimentary.	
Computer Trouble	Computer Trouble	System		
Conferenced Call		Intercom	Generated if a call is conferenced together with another call.	
Congestion	Congestion	Video	Generated when the user-specified level and pattern of congestion is detected within a region of interest.	
Congestion Restored	Congestion Restored	Video	Generated 8 seconds after last detection of a Congestion event.	
Controller Connection Mismatch	Controller Connection Mismatch	System	Generated when the OnGuard attempts to make a connection to a controller by upgrading or degrading the connection while the controller is online.	

Alarm	Event	Event Type	Description	Duress*
Controller Encryption Error	Controller Encryption Error	System	Generated in several instances, including when: • A controller is configured for a plain connection when it requires encryption. • An encrypted controller is online, but its configuration is changed to a plain connection. • A controller is configured for a plain connection, but then a physical controller swap is made where the new controller requires encryption. • A controller that supports encryption is currently online with a plan connection, and then the DIR switch 8 is turned on.	
CPU Data Error	CPU Data Error	System	A CPU data error was detected.	
CPU Utilization Threshold Exceeded	CPU Utilization Threshold Exceeded	System	Generated by an LNVR recorder when current CPU level exceeds the user defined limit.	
CPU Utilization Threshold Restored	CPU Utilization Threshold Restored	System	Generated by an LNVR recorder when the current CPU level drop below the user defined limit.	
Credit Card Tendered	Credit Card Tendered	POS	Generated when a credit card was used as tender.	
Cross Zone Trouble	Cross Zone Trouble	Trouble		
Current Time	Current Time	POS	An event that reports the current time.	

Alarm	Event	Event Type	Description	Duress*
Database Error Event Polling Stopped	Database Error Event Polling Stopped	System	Generated by the communication server when there is a problem writing events to the database. This event is not written to the database but is sent to Alarm Monitoring clients. Polling of the events from the various hardware devices is stopped until the events can be written to the database.	
Database Error in Panel Download	Database Error in Panel Download	System	Generated by the communication server when the database cannot be opened at the start of a database download to a controller.	
Data Lost	Data Lost	System	The dialer data has been lost and there is a transmission error.	
Date Changed	Date Changed	System	The date was changed.	
Day Trouble	Day Trouble	Trouble	A day trouble condition has been detected.	
Day Trouble Restore	Day Trouble Restore	Trouble	A day trouble condition has been restored.	
Day/Night Alarm	Day/Night Alarm	Trouble	A day/night alarm condition has been detected.	
Day/Night Alarm Restore	Day/Night Alarm Restore	Trouble	A day/night alarm condition has been restored.	
Daylight Saving Time Audit	Daylight Saving Time Audit	System	Start of DST (Daylight Saving Time) or end of DST has occurred.	
Deactivate Output	Deactivate Output	System		
Dealer ID	Dealer ID	System		
Debit, ATM, Check Card Tender	Debit, ATM, Check Card Tender	POS	Transaction that indicated that a debit, ATM, or check card was used as tender.	
Deferred Close	Deferred Close	Open/ Close		

Alarm	Event	Event Type	Description	Duress*
Deferred Open/Close	Deferred Open/ Close	Open/ Close		
Denied, Badge Not in Panel	Denied, Badge Not in Panel	Denied	Generated when a badge is denied at a reader because it is not in the system.	Yes
Denied Count Exceeded	Denied Count Exceeded	Denied		Yes
Denied Low Battery	Denied Low Battery	Denied	Generated when access is denied because the battery on the device is low.	
Denied, No Command Authority	Denied, No Command Authority	Denied	Generated when a reader command function was denied because the user did not have the command authority to execute the function.	
Denied - No Host Approval	Denied - No Host Approval	Denied	Generated when access was denied because the host did not grant approval. This can happen because the host response did not come back in a timely fashion or the controller is offline with the host.	Yes
Denied, Not Authorized	Denied, Not Authorized	Denied	Generated when access was denied because user authorization did not match authorization assigned to the reader (lock).	
Denied, PIN Only Request	Denied, PIN Only Request	Denied	Generated when access was denied for a pin only request (either an invalid pin code or pin support is not enabled for the panel).	Yes
Denied - Unauthorized Assets	Denied - Unauthorized Assets	Denied	Generated when access was denied because of unauthorized assets.	Yes
Denied Under Duress	Access Denied Under Duress	Duress	Generated when the cardholder was denied access under duress.	Yes

Alarm	Event	Event Type	Description	Duress*
Denied Unmask, Active Zones in Group	Denied Unmask - Active Zones in Group	Denied	Generated when the unmask command failed because there are still active zones in the group.	
Deny Count Exceeded	Deny Count Exceeded	Denied	Generated when a specified number of invalid attempts are made in a row at a reader.	
Deposit Amount Paid Pending Purchase	Deposit Amount Paid Pending Purchase	POS	Event indicating that a deposit amount paid pending purchase has occurred.	
Deposit Return	Deposit Return	POS	Transaction for a deposit return.	
Detector High Sensitivity	Detector High Sensitivity	Trouble	A detector high sensitivity condition has been detected.	
Detector High Sensitivity Restore	Detector High Sensitivity Restore	Trouble	A detector high sensitivity condition has been restored.	
Detector Low Sensitivity	Detector Low Sensitivity	Trouble	A detector low sensitivity condition has been detected.	
Detector Low Sensitivity Restore	Detector Low Sensitivity Restore	Trouble	A detector low sensitivity condition has been restored.	
Detector Test	Detector Test	Fire	Generated when the fire detection test is initiated.	
Detector Test Fail	Detector Test Fail	Fire	Generated when the fire detection test fails.	
Detector Test OK	Detector Test OK	Fire	Generated when the fire detection test is successfully completed.	
Device Turned Off	Device Turned Off	Trouble	A device turned off.	
Device Turned On	Device Turned On	Trouble	A device turned on.	
Device Type Mismatch	Device Type Mismatch	System	Generated when the device is of a different type than what it has been configured for.	

Alarm	Event	Event Type	Description	Duress*
Diagnostic	Diagnostic	System	A diagnostic report was requested.	
Diagnostic Error	Diagnostic Error	System	A device is reporting a diagnostic error.	
Dial Out Method	Dial Out Method	System		
Dialer Disabled	Dialer Disabled	Trouble	The dialer has become disabled.	
Dialer Disabled Restore	Dialer Disabled Restore	Trouble	The dialer has been restored from being disabled.	
Dialer Shutdown	Dialer Shutdown	Trouble	The dialer has shutdown.	
Dialing Error	Dialing Error	Trouble	An error has been detected when dialing.	
Dialup Last Connection Time Expired	Dialup Last Connection Time Expired	System	Generated by the communication server for dialup panels that have exceeded the set number of hours since their last connection. When this event is generated, the communication server will attempt to connect to the panel. If the dialup panel repeatedly receives this event, the panel should be investigated to see why it is not calling back.	
Dialup Stored Command Limit Exceeded	Dialup Stored Command Limit Exceeded	System	Generated by the communication server for dialup panels that have exceeded their stored command limit. When this event is generated, the communication server will attempt to connect to the panel. If the dialup panel repeatedly receives this event, the panel should be investigated to see why it is not calling back.	
Digital Dialer Daily Test Fail	Digital Dialer Daily Test Fail	System	Digital dialer failed to report its daily test.	
Disable Intercept Mode	Disable Intercept Mode	System		

Alarm	Event	Event Type	Description	Duress*
Directional Motion	Directional Motion	Video	Generated when an object moving in a pre-specified direction is detected.	
Directional Motion Restored	Directional Motion Restored	Video	Generated 8 seconds after last detection of a Directional Motion event.	
Disarm From Alarm	Disarm From Alarm	System	An account in alarm was reset/disarmed.	
Discount Entered as Absolute Amount	Discount Entered as Absolute Amount	POS	Generated when a discount was entered as an absolute amount.	
Discount Entered as Percentage	Discount Entered as Percentage	POS	Generated when a discount was entered as a percentage.	
Disk Read Utilization Threshold Exceeded	Disk Read Utilization Threshold Exceeded	System	Generated by an LNVR recorder when current hard drive read speed exceeds the user defined limit.	
Disk Read Utilization Threshold Restored	Disk Read Utilization Threshold Restored	System	Generated by an LNVR recorder when the current hard drive read speed drops below the user defined limit.	
Disk Write Utilization ThresholdExceeded	Disk Write Utilization Threshold Exceeded	System	Generated by an LNVR recorder when current hard drive write speed exceeds the user defined limit.	
Disk Write Utilization Threshold Restored	Disk Write Utilization Threshold Restored	System	Generated by an LNVR recorder when the current hard drive write speed drops below the user defined limit.	
Door Close	Door Close	System	Generated when a door closes.	
Door Contact Tamper Active	Door Contact Tamper	System	Generated when the door contact tamper has gone active.	
Door Contact Tamper Restored	Door Contact Tamper Cancelled	System	Generated when the door contact tamper has been restored.	

Alarm	Event	Event Type	Description	Duress*
Door Cycled	Door Cycled	System	Generated when momentary access is granted to a door. This is a temporary door state in which the door initiates the door sequence as if a valid card was read. Door cycled cannot be scheduled.	
Door Forced	Door Forced	Trouble	The door was forced open without an access request.	
Door Forced Open	Door Forced Open	System	Generated when a “Door Forced Open” condition has been detected.	
Door Forced Open Masked	Door Forced Open Masked	System	Generated when the “Door Forced Open” event has become masked for the device.	
Door Forced Open Restored	Door Forced Open Cancelled	System	Generated when a “Door Forced Open” condition has been restored.	
Door Forced Open Unmasked	Door Forced Open Unmasked	System	Generated when the “Door Forced Open” event has become unmasked for the device.	
Door Forced Trouble	Door Forced Trouble	Trouble	An access point has been forced open in an unarmed area.	
Door Held Open	Door Held Open	System	Generated when a “Door Held Open” condition has been detected.	
Door Held Open Masked	Door Held Open Masked	System	Generated when the “Door Held Open” event has become masked for the device.	
Door Held Open Restored	Door Held Open Cancelled	System	Generated when a “Door Held Open” condition was restored.	
Door Held Open Unmasked	Door Held Open Unmasked	System	Generated when the “Door Held Open” event has become unmasked for the device.	
Door Left Open	Door Left Open	Trouble	An access point was open when the door cycle time expired.	

Alarm	Event	Event Type	Description	Duress*
Door Left Open Alarm	Door Left Open Alarm	Trouble	An open access point was open when the open time expired in an armed area.	
Door Left Open Restore	Door Left Open Restore	Trouble	An access point in a door left open state has restored.	
Door Left Open Trouble	Door Left Open Trouble	Trouble	An open access point was open when the open time expired in an unarmed area.	
Door Locked	Door Locked	Trouble	Generated when a door returns to its normal door state (locked). When a door is in the lock door state, you can initiate the door sequence using schedules, command center functions, door requests, or valid card requests. Door locked is similar to a reader being in card and pin mode.	
Door Open	Door Open	System	An event indicating that the door has opened.	
Door Open From Inside	Door Open From Inside		Door opened from inside, only when not in unlocked mode.	
Door Request	Door Request	System	This event is generated from Bosch intrusion panels when a door is manually activated to open without the presentation of an ID.	
Door Restore	Door Restore	Trouble	An access alarm/trouble condition has been eliminated.	
Door Secured	Door Secured	System	Generated when no access is allowed to a door. When a door is in a secure state, no access is allowed through the door until it is returned to the locked state. Door secured is similar to a reader being in locked mode.	

Alarm	Event	Event Type	Description	Duress*
Door Shunt Command Executed From Reader	Door Shunt Command Executed From Reader	System	Generated when the door shunt command was executed from the reader.	
Door Shunt Command Results - Cancelled	Door Shunt Command Results - Cancelled	System	Generated when the door is closed while the door shunt command is executing.	
Door Station	Door Station	Trouble	Identified door for next report.	
Door Unlocked	Door Unlocked	System	Generated when there is free access to a door. When a door is unlocked, the door is shunted and the strike does not prevent the door from opening. In this state, you do not need to activate a door request or present a valid card to gain access. Door unlocked is similar to a reader being in unlocked mode.	
Drift Compensation Error	Drift Compensation Error	Trouble		
Driver Error in Panel Download	Driver Error in Panel Download	System	Generated by the communication server when an error occurs during a database download to a controller.	
Duct Alarm	Duct Alarm	Trouble	A duct alarm condition has been detected.	
Duct Alarm Restore	Duct Alarm Restore	Trouble	A duct alarm condition has been restored.	
Duress Access Grant	Duress Access Grant	Duress		
Duress Egress Grant	Duress Egress Grant	Duress		
DURESS - Interlock Area Busy	DURESS - Interlock Area Busy	Duress	Access was requested to an interlocked area while under duress.	Yes

Alarm	Event	Event Type	Description	Duress*
Egress Denied	Egress	Egress	A user presented a badge to an out reader (reader leaving the area) and was denied access.	
Egress Granted	Egress	Egress	A user presented a badge to an out reader (reader leaving the area), was granted access and opened the door after the grant.	
Elevator Terminal Mode Access to Authorized Floors	Elevator Terminal Mode Access to Authorized Floors	System	Generated when the elevator terminal mode has changed to “Access to Authorized Floors.”	
Elevator Terminal Mode Default Floor	Elevator Terminal Mode Default Floor	System	Generated when the elevator terminal mode has changed to “Default Floor Only.”	
Elevator Terminal Mode Default Floor or User Entry of Destination Floor	Elevator Terminal Mode Default Floor or User Entry of Destination Floor	System	Generated when the elevator terminal mode has changed to “Default Floor or User Entry of Destination Floor.”	
Elevator Terminal Mode User Entry of Destination Floor	Elevator Terminal Mode User Entry of Destination Floor	System	Generated when the elevator terminal mode has changed to “User Entry of Destination Floor.”	
Embedded Analytics Failure	Embedded Analytics Failure	System	Generated when embedded analytics fail to initialize.	
Embedded Analytics Restored	Embedded Analytics Restored	System	Generated when embedded analytics initialize successfully following a failure.	
Employee Sign Off	Employee Sign Off	POS	Generated when an employee signs off.	
Employee Sign On	Employee Sign On	POS	Generated when an employee signs on.	
Exit Request Denied: Interlock Area Busy	Exit Request Denied: Interlock Area Busy	Area Control	A request to exit made via REX button was denied because a door is open or the door strike is active within an interlocked area.	

Alarm	Event	Event Type	Description	Duress*
Extended Held Command Denied	Extended Held Command Denied	System	Generated when an extended held command is denied.	
Extended Held Command Set From Reader	Extended Held Command Set From Reader	System	Generated when an extended held command is entered at the reader.	
Extended Held Open Mode Disabled	Extended Held Open Mode Disabled	System	Generated when extended held open mode is disabled.	
Extended Held Open Mode Enabled	Extended Held Open Mode Enabled	System	Generated when extended held open mode is enabled.	
Facial Detection	Facial Detection	Video	Generated when one or several faces are detected.	
Facial Detection Restored	Facial Detection Restored	Video	Generated 8 seconds after last detection of a face.	
Facility Code Only Mode Denied: Blocked Mode	Facility Code Only Mode Denied: Blocked Mode	System	Automatic scheduled change to facility code only mode was denied because lock is in blocked mode.	
Facility Code Only Mode Denied: Secured Mode	Facility Code Only Mode Denied: Secured Mode	System	Automatic scheduled change to facility code only mode was denied because lock is in secured mode.	
Facility Occupancy Too Low	Facility Occupancy Too Low	Video	Generated when the occupancy falls below the user-specified limit.	
Facility Occupancy Too Low Restored	Facility Occupancy Too Low Restored	Video	Generated when the occupancy returns to a value above the lower limit.	
Facility Occupancy Too High	Facility Occupancy Too High	Video	Generated when the occupancy rises above the user-specified limit.	
Facility Occupancy Too High Restored	Facility Occupancy Too High Restored	Video	Generated when the occupancy returns to a value below the upper limit.	

Alarm	Event	Event Type	Description	Duress*
Failed to Report Expected Event	Failed to Report Expected Event	System	Generated when a device that is supposed to report an event within a certain period of time fails to report an event during this time period.	
Fire Alarm	Fire Alarm	Fire	Generated when a fire device is in alarm.	
Fire Alarm Acknowledge	Fire Alarm Acknowledge	Fire	Generated when a fire alarm has been acknowledged.	
Fire Alarm Acknowledged Clear	Fire Alarm Acknowledged Clear	Fire	Generated when a fire alarm has been acknowledged and cleared.	
Fire Alarm Block Acknowledge	Fire Alarm Block Acknowledge	Fire	Generated when all fire alarms have been acknowledged at the fire panel.	
Fire Alarm In	Fire Alarm In	Fire	Generated when a new fire alarm has been detected for the device.	
Fire Alarm Out	Fire Alarm Out	Fire	Generated when a device with a previous fire alarm has returned to its normal state.	
Fire Button Set	Fire Button Set	Fire	The reported fire button has been set.	
Fire Missing	Fire Missing	Fire		
Fire Walk Test Ended	Fire Walk Test Ended	Fire	A fire walk test has ended.	
Fire Walk Test Started	Fire Walk Test Started	Fire	A fire walk test has started.	
Fire Zone Walk Tested	Fire Zone Walk Tested	Fire	A fire zone has been tested.	
Firmware Download Started	Firmware Download Started	System	Generated when the firmware download has started.	
Firmware Download Completed	Firmware Download Completed	System	Generated when the firmware download has completed.	

Alarm	Event	Event Type	Description	Duress*
Firmware Download Failed	Firmware Download Failed	System	Generated when the firmware download has failed.	
First Card Unlock Mode Denied: Blocked Mode	First Card Unlock Mode Denied: Blocked Mode	System	Automatic scheduled change to first card unlock mode was denied because lock is in blocked mode.	
First Card Unlock Mode Denied: Secured Mode	First Card Unlock Mode Denied: Secured Mode	System	Automatic scheduled change to first card unlock mode was denied because lock is in secured mode.	
First Card Unlock Mode Disabled	First Card Unlock Mode Disabled	System	Generated when first card unlock mode is disabled for a door.	
First Card Unlock Mode Enabled	First Card Unlock Mode Enabled	System	Generated when first card unlock mode is enabled for a door.	
Foil Break Alarm	Foil Break Alarm	Trouble	Generated when a break in a foil circuit occurs. This is most commonly used to trigger an alarm when glass being protected with the foil circuit is broken.	
Foil Break Restore	Foil Break Restore	Trouble	Generated when a foil break alarm condition has been restored.	
Foodstamps Tender	Foodstamps Tender	POS	Indicates that food stamps were used as tender.	
Gasoline Prepayment	Gasoline Prepayment	POS	Transaction for a gasoline prepayment	
Gasoline Prepayment Refund	Gasoline Prepayment Refund	POS	Transaction for a gasoline prepayment	
Generic Event	Generic Event	Generic	A generic event exists with more specific information in the event text.	
Global Linkage Action Executed	Global Linkage Action Executed	System	Generated when a global I/O linkage has executed.	
Global Linkage Action Failed	Global Linkage Action Failed	System	Generated when a global I/O linkage has failed.	

Alarm	Event	Event Type	Description	Duress*
Granted Access	Access Granted	Granted	Generated when access was granted.	
Granted APB Violation, Entry Made	Access Granted Anti-Passback Used	Area Control	Generated when an anti-passback violation occurred but access was granted and entry was made. This can happen when using soft anti-passback.	
Granted APB Violation, No Entry Made	Access Granted Anti-Passback Not Used	Area Control	Generated when an anti-passback violation occurred and access was granted but no entry was made. This can happen when using soft anti-passback.	
Granted Facility Code	Access Granted On Facility Code	Granted	Generated when access was granted based on a valid facility code.	
Granted Facility Code, No Entry	Access Granted On Facility Code No Entry Made	Granted	Generated when access was granted on facility code but no entry was made at the door.	
Granted No Entry	Access Granted No Entry Made	Granted	Generated when access was granted but no entry was made at the door.	Yes
Granted Under Duress	Access Granted Under Duress	Emergency	Generated when the cardholder was granted access under duress.	
Granted Under Duress, No Entry	Access Granted Under Duress - No Entry Made	Emergency	Generated when the cardholder was granted access under duress but no entry was made.	
Grounded Loop Active	Grounded Loop Alarm Active	System	Generated when a grounded loop fault condition has been detected.	
Grounded Loop Restored	Cancelled Grounded Loop	System	Generated when the grounded loop fault condition was restored.	
Guard Tour Action Executed	Guard Tour Action Executed	System	Generated when a guard tour action has executed.	
Guard Tour Action Failed	Guard Tour Action Failed	System	Generated when a guard tour action has failed.	

Alarm	Event	Event Type	Description	Duress*
History Report End	History Report End	System		
History Report Start	History Report Start	System		
Hold	Hold	Intercom	Generated when a phone call is placed on hold.	
Holdup Alarm Restore	Holdup Alarm Restore	Emergency	Holdup alarm was restored.	
Host Executed Function List	Host Executed Function List	System	Generated when a function list has been executed from the host.	
Host Open Door - Door Used	Host Open Door - Door Not Used	System	When the host issued an open door command and the door was opened.	
Host Open Door - Door Not Used	Host Open Door - Door Not Used	System	When the host issued an open door command and the door was not opened.	
In-Camera-Memory Download Completed	In-Camera-Memory Download Completed	System	Generated when the process of retrieving the files from the camera memory is completed.	
In-Camera-Memory Download Failed	In-Camera-Memory Download Failed	System	Generated when the process of retrieving the files from the camera memory is failed.	
In-Camera-Memory Download Restored	In-Camera-Memory Download Restored	System	Generated when the process of retrieving the files from the camera memory is restored.	
In-Camera-Memory Download Started	In-Camera-Memory Download Started	System	Generated when the process of retrieving the files from the camera memory is started.	
Inactive Badge	Inactive Badge	Denied	Generated when access was denied because the badge was inactive.	Yes
Incoming Call	Incoming Call	Intercom	Generated when there is an incoming call.	
Information Message	Information Message	POS	Used to report information messages	
Initiated	Initiated	Intercom	Generated when a phone call is initiated.	

Alarm	Event	Event Type	Description	Duress*
Input Bypassed	Input Bypassed	System	Generated when an input has been temporarily bypassed from detecting changes in state and reporting alarms. Typically, you would specify to bypass the input in order to troubleshoot an input issue without reporting the alarms for it. This is often done during an armed state. After the system enters the disarmed state, the input normally leaves the bypassed state.	
Input Disabled	Input Disabled	System	This is similar to Input Bypassed except the input has been permanently disabled from detecting and reporting activity until the operator specifically enables it.	
Input Masked	Input Masked	System	Generated when an input has become masked.	
Input Restored	Input Restored	System	An input has been returned to the normal mode of operation after being in either a bypassed or disabled state.	
Input Unmasked	Input Unmasked	System	Generated when an input has become unmasked.	
Intercom Function	Intercom Function	Intercom	Generated when an intercom function has been executed.	
Interlock Area Busy	Interlock Area Busy	Area Control	Access requested by presenting a badge was denied because a door is open or the door strike is active within an interlocked area.	

Alarm	Event	Event Type	Description	Duress*
Insufficient Frame Rate Detected	N/A	N/A	This warning appears when the analytics are not receiving the required minimum frame rate for the events configured on the video channel.	
Insufficient Frame Rate Restored	N/A	N/A	Generated when the frame rate reaches a value sufficient for the events configured on the video channel.	
Intrusion Command Accepted	Intrusion Command Accepted	Generic	An intrusion command was successfully executed.	
Intrusion Command Denied	Intrusion Command Denied	Denied	An attempt to execute an intrusion command was denied, either the command is not allowed at the reader, the user is not authorized for this command, or invalid command arguments were supplied.	
Invalid Access Level	Invalid Access Level	Denied	Generated when access was denied because of an invalid access level.	Yes
Invalid Badge	Invalid Badge	Denied	Generated when access was denied because the badge ID was unknown to the controller.	Yes
Invalid Camera	Invalid Camera	Video	Generated when the camera is tampered with (covered, moved, or out-of-focus).	
Invalid Camera Restored	Invalid Camera Restored	Video	Generated 8 seconds after the camera becomes valid again or in the case of camera covered or moved, when the background is relearned.	
Invalid Card Format	Invalid Card Format	Denied	Generated when the badge contained a card format that was not recognized by the reader.	

Alarm	Event	Event Type	Description	Duress*
Invalid Device Serial Number	Invalid Device Serial Number	System	Generated when the device does not have a valid serial number.	
Invalid Facility Code	Invalid Facility Code	Denied	Generated when access was denied because the badge had an invalid facility code.	Yes
Invalid Issue Code	Invalid Issue Code	Denied	Generated when access was denied because the issue code read from the badge did not match the current issue code stored in the database for the badge.	Yes
Invalid OEM Code	Invalid OEM Code	System	Indicates that the hardware did not contain the expected OEM (Original Equipment Manufacturer) code.	
Invalid PIN Number	Invalid PIN Number	Denied	Generated when access was denied because an invalid PIN was entered.	Yes
Item Correct of Previously entered Item	Item Correct of Previously entered Item	POS	Generated to indicate that an item was corrected.	
Item Sold	Item Sold	POS	Indicates an item was sold.	
IVS Channel Processing Failed	IVS Channel Processing Failed	Video	Generated by the IntelligentVideo Server when video processing is terminated due to an error or lost connection.	
IVS Channel Processing Restarted	IVS Channel Processing Restarted	Video	Generated when the IntelligentVideo Server re-establishes a connection to a channel that previously reported failure.	
IVS Connection Lost	IVS Connection Lost	Video	Generated when the camera is configured to analyze video on a remote IntelligentVideo Server and connection to the IntelligentVideo Server is lost.	

Alarm	Event	Event Type	Description	Duress*
IVS Connection Restored	IVS Connection Restored	Video	Generated when the connection to the IntelligentVideo Server was lost and has been restored.	
IVS Engine Connection Lost	IVS Engine Connection Lost	Video	Generated when the IntelligentVideo Server looses connection to the LpsSearchSvc service and video processing of all channels fails.	
IVS Engine Connection Restored	IVS Engine Connection Restored	Video	Generated when the IntelligentVideo Server reconnects to the LpsSearchSvc service after the connection has been lost.	
Key Override	Key Override	System	Generated when the key override is used in a Mortise lockset. Not supported in Cylindrical lockset.	
Keypad Fire	Keypad Fire	Fire	A fire alarm has been generated from a keypad.	
Lamp Test Activated	Lamp Test Activated	Fire	Generated when the lamp test is activated. When a lamp test is activated the AM-2020 will send out a command sequence to display a set of solid blocks on the hardware's LCD.	
Lamp Test Completed	Lamp Test Completed	Fire	Generated when the lamp test successfully completes.	

Alarm	Event	Event Type	Description	Duress*
License Will Soon Expire - X Days Left	License Will Soon Expire - X Days Left	System	Generated when the system license is reaching its expiration date. This alarm is dependent on linkage server being configured and running on a host workstation. It is advised that this alarm be configured to be e-mailed to the system administrator. For more information, see the Acknowledge Alarms chapter in the Alarm Monitoring user guide. **Note:** In order for the alarm to be reported to monitoring stations there must be at least one panel configured and marked online. The panel does not need to exist or actually be online in Alarm Monitoring, it simply needs to exist in the System Status view. **Note:** This event must be available as an input event to use the Global I/O output action. Make sure it is available to be sent out via DataConduIT.	
Line Error Active	Line Error Active	System	Generated when a line error fault condition has been detected.	
Line Error Restored	Cancelled Line Error	System	Generated when the line error fault condition was restored.	

Alarm	Event	Event Type	Description	Duress*
Local I/O Executed Function List	Local I/O Executed Function List	System	Generated when a local I/O function list has been activated.	
Loitering	Loitering	Video	Generated when a loiterer is detected.	
Loitering Restored	Loitering Restored	Video	Generated 8 seconds after the last detection of a Loitering event.	
Lock Initialized	Lock Initialized	System	Lock was initialized using the PP (Portable Programmer) application.	
Lock Updated	Lock Updated	System	Lock was updated.	
Lock Powered Up by Portable Programmer	Lock Powered Up by Portable Programmer	System	Generated after a power up by the portable programmer.	
Locked Under AFC	Locked Under AFC	System	End of AFC state.	
Locked Under First Card Unlock	Locked Under First Card Unlock	System	First card unlock mode; door is relocked.	
Lottery Pay Out	Lottery Pay Out	POS	Generated when a lottery pay out has occurred.	
Low Battery	Low Battery	System	Low battery alarm.	
Low Battery Restored	Low Battery Restored	System	Generated when a low battery is restored.	
Lottery Sale	Lottery Sale	POS	Generated when an event for a lottery sale has occurred.	
Low Voltage	Low Voltage	System	Generated when a low voltage condition has been detected at the device.	
Low Voltage Restored	Low Voltage Restored	System	Generated when a device resumes its proper voltage.	
Manufacturer Coupon	Manufacturer Coupon	POS	Indicates a manufacturer coupons.	
Manufacturer Coupon Redemption	Manufacturer Coupon Redemption	POS	Transaction generated for a manufacturer coupon redemption.	

Alarm	Event	Event Type	Description	Duress*
Max Assets Reached	Max Assets Reached	System	Generated during a download when the number of assets exceeds the maximum value configured for the controller. Only the maximum number of assets will be downloaded (all others will be ignored).	
Max Biometric Templates Reached	Max Biometric Templates Reached	System	Generated during a download when the number of biometric templates exceeds the maximum value configured for the controller. Only the maximum number of templates will be downloaded (all others will be ignored).	
Max Cardholders Reached	Max Cardholders Reached	System	Generated during a download when the number of cardholders exceeds the maximum value configured for the controller. Only the maximum number of cardholders will be downloaded (all others will be ignored).	
Merchandise Returned	Merchandise Returned	POS	Generated when merchandise is returned.	
Miscellaneous Tender	Miscellaneous Tender	POS	Generated when miscellaneous tender is used.	
Module Active	Module Active	Fire	Generated when a monitor or control module connected to the system becomes active. The device label assigned to this device and the zone label assigned to the first zone programmed for this device will be included with the event.	

Alarm	Event	Event Type	Description	Duress*
Module Clear	Module Clear	Fire	Generated when a monitor or control module connected to the system is no longer active. The device label assigned to this device and the zone label assigned to the first zone programmed for this device will be included with the event.	
Motion Detected (AI)	Motion Detected (AI)	Video	Generated when motion has been detected on a given input channel (camera). Motion is considered any change in the environment within the field of view of the camera.	
Motion Detected (AI) Restored	Motion Detected (AI) Restored	Video	Generated when motion has been restored (is no longer detected) on a given input channel (camera). Motion is considered any change in the environment within the field of view of the camera.	
Muster Mode Reset	Muster Mode Reset	Mustering	Generated when muster mode is reset.	
Muster Mode Start	Muster Mode Start	Mustering	Generated when muster mode is started.	
Negative Tax	Negative Tax	POS	Generated when negative tax is used.	
Negative Total	Negative Total	POS	Generated when there is a negative total.	
Network Utilization Threshold Exceeded	Network Utilization Threshold Exceeded	System	Generated by an LNVR recorder when current Network activity levels exceeds the user defined limit.	
Network Utilization Threshold Restored	Network Utilization Threshold Restored	System	Generated by an LNVR recorder when the current Network activity level dropped below the user defined limit.	

Alarm	Event	Event Type	Description	Duress*
No Biometric Template Data	No Biometric Template Data	Biometric	Generated when no biometric template data was available from the biometric reader at the end of a verification sequence.	
No Blocking Override	No Blocking Override		User does not have Blocked override privilege.	
Non-Fire Active	Non-Fire Active	System	An event indicating a non fire related alarm condition is active.	
Non-Fire Active Cleared	Non-Fire Active Cleared	System	An event indicating a non fire related alarm condition is no longer active.	
Not Configured	Not Configured	System	Generated when a device has not been configured or defined by the host.	
No Sale	No Sale	POS	Transaction generated for a no sale.	
Object Crosses a Region	Object Crosses a Region	Video	Generated when an object is detected in the process of crossing a user-specified region.	
Object Crosses a Region Restored	Object Crosses a Region Restored	Video	Generated 8 seconds after the last detection of an Object Crosses a Region event.	
Object Detection	Object Detection	Video	Generated when an object complying with user-specifications is detected.	
Object Detection Restored	Object Detection Restored	Video	Generated 8 seconds after the last detection of an Object Detection event.	
Object Left Behind	Object Left Behind	Video	Generated when a foreground object is left for more than a pre-specified duration.	

Alarm	Event	Event Type	Description	Duress*
Object Left Behind Restored	Object Left Behind Restored	Video	Generated when the left object was taken or the background (after a certain time interval) is relearned.	
Object Lurking	Object Lurking	Video	Generated when a moving object stops or slows down for at least 7 seconds.	
Object Lurking Restored	Object Lurking Restored	Video	Generated 8 seconds after the last detection of an Object Lurking event.	
Object Moves Too Fast	Object Moves Too Fast	Video	Generated when a moving object is detected in a scene with a speed that exceeds the user-specified rate.	
Object Moves Too Fast Restored	Object Moves Too Fast Restored	Video	Generated 8 seconds after the last detection of an Object Moves Too Fast event.	
Object Starts to Move	Object Starts to Move	Video	Generated when a monitored object begins moving.	
Object Starts to Move Restored	Object Starts to Move Restored	Video	Generated 8 seconds after last detection of an Object Starts to Move event.	
Object Removed	Object Removed	Video	Generated when a background object is removed.	
Object Removed Restored	Object Removed Restored	Video	Generated when the object is returned to its original location or the background (after a certain time interval) is relearned.	
Object Stops	Object Stops	Video	Generated when a foreground object stops.	
Object Stops Restored	Object Stops Restored	Video	Generated 8 seconds after the last detection of an Object Stops event.	

Alarm	Event	Event Type	Description	Duress*
Open Door Command Issued - Door Used	Open Door Command Issued - Door Used	System	Indicates that a command was issued to open the door and the door was used. This can be for a locally generated open door command or one from the host.	
Open Door Command Issued - Door Not Used	Open Door Command Issued - Door Not Used	System	Indicates that a command was issued to open up the door and the door was not used. This can be for a locally generated open door command or one from the host.	
Open Line Active	Open Line Active	System	Generated when an open line fault condition has been detected.	
Open Line Restored	Cancelled Open Line	System	Generated when the open line fault condition was restored.	
Override Preprogrammed Price	Override Preprogrammed Price	POS	Generated when the preprogrammed price is overridden.	
Panel Download Completed	Full Panel Download Completed	System	Generated when a database download to the controller has completed.	
Panel Download Started	Full Panel Download Started	System	Generated when a database download to the controller has started.	
Panel Event Capacity Exceeded - Events Overwritten	Panel Event Capacity Exceeded - Events Overwritten	System	Generated when the event log in the panel fills up and starts overwriting old events.	
Panel Free Memory Low	Panel Free Memory Low	System	Generated when the free memory in the panel (controller) is below what is determined to be a safe value.	

Alarm	Event	Event Type	Description	Duress*
Panel ID Mismatch	Panel ID Mismatch	System	Generated when the panel (controller) has a different ID than what is in the database. This can happen if a new panel or replacement panel is placed out in the field. A download to the panel should correct the problem.	
Panel Marked Offline After Timeout	Panel Marked Offline After Timeout	System	Generated when the video recorder is automatically placed offline because a connection cannot be made after the user specified amount of time.	
Panel Options Mismatch	Panel Options Mismatch	System	Generated when the options inside of the panel differ from what the panel is currently configured for in the database. This can happen if the panel options change and a download is not issued to the panel. To correct this situation, a download should be issued to the panel.	
Panel Power Up Complete	Panel Power Up Complete	System	Generated when the panel power up is complete.	
Panic Abort	Panic Abort	Trouble	Generated when a panic alarm has been manually aborted/canceled.	
Panic Alarm	Panic Alarm	Trouble	Generated when emergency assistance has been manually requested.	
Panic Alarm Restore	Panic Alarm Restore	Trouble	Generated when the panic alarm has been restored.	
Pay Out	Pay Out	POS	Generated when a payout takes place.	
Payment of Refund to Customer	Payment of Refund to Customer	POS	Generated when a payment or refund is given to a customer.	

Alarm	Event	Event Type	Description	Duress*
Payment Toward Charge Account Balance	Payment Toward Charge Account Balance	POS	Generated when a payment toward an account balance.	
People Counting	People Counting	Video	Generated when the count was updated (usually within a short delay after an individual passes).	
People Entry Rate Too High	People Entry Rate Too High	Video	Generated when the number of entering people rises above the limit during the specified time interval.	
People Entry Rate Too High Restored	People Entry Rate Too High Restored	Video	Generated when the number of entering people returns to a value below the limit during the specified time interval.	
People Entry Rate Too Low	People Entry Rate Too Low	Video	Generated when the number of entering people falls below the limit during the specified time interval.	
People Entry Rate Too Low Restored	People Entry Rate Too Low Restored	Video	Generated when the number of entering people returns to a value above the limit during the specified time interval.	
People Exit Rate Too High	People Exit Rate Too High	Video	Generated when the number of exiting people rises above the limit during the specified time interval.	
People Exit Rate Too High Restored	People Exit Rate Too High Restored	Video	Generated when the number of exiting people returns to a value below the limit during the specified time interval.	
People Exit Rate Too Low	People Exit Rate Too Low	Video	Generated when the number of exiting people falls below the limit during the specified time interval.	
People Exit Rate Too Low Restored	People Exit Rate Too Low Restored	Video	Generated when the number of exiting people returns to a value above the limit during the specified time interval.	

Alarm	Event	Event Type	Description	Duress*
Pick Up	Pick Up	POS	Transaction indicating a pick up has occurred.	
Point Enabled	Point Enabled	System		
Point Disabled	Point Disabled	System		
Poor Video Visibility Restored	N/A	N/A	Generated when the video quality returns to an acceptable level.	
Power Failure Active	Power Failure	System	Generated when a power failure condition has been detected.	
Power Failure Restored	Cancelled Power Failure	System	Generated when the power failure condition was restored.	
Pre-Alarm	Pre-Alarm	System	An event indicating a pre-alarm condition is active.	
Pre-Alarm Clear	Pre-Alarm Clear	System	An event indicating a pre-alarm condition is no longer active.	
Price Lookup	Price Lookup	POS	Generated when a price lookup has taken place.	
Quantity or Weight	Quantity or Weight	POS	An event indicating a quantity or weight.	
Reader Input Tamper Active	Reader Input Tamper	System	Generated when the reader input tamper has gone active.	
Reader Low Battery	Reader Low Battery	System	Reader low battery alarm.	
Reader Low Battery Restored	Reader Low Battery Restored	System	Generated when a reader low battery is restored.	
Reader Input Tamper Restored	Reader Input Tamper Cancelled	System	Generated when the reader input tamper was restored.	
Reader Mode Blocked	Reader Mode Blocked	System	Lock has entered blocked mode.	
Reader Mode Secured	Reader Mode Secured	System	Lock has entered secured mode.	
Reader Mode Unsecured	Reader Mode Unsecured	System	Lock has entered unsecured mode.	

Alarm	Event	Event Type	Description	Duress*
Reader Mode Card and Pin	Reader Mode Card and Pin	System	Generated when the reader mode has changed to “Pin and Card” for the device.	
Reader Mode Card Only	Reader Mode Card Only	System	Generated when the reader mode has changed to “Card Only.”	
Reader Mode Facility Code	Reader Mode Facility Code	System	Generated when the reader mode has changed to “Facility Code Only.”	
Reader Mode First Card Unlock	Reader Mode First Card Unlock	System	Generated when the reader mode has changed to “First Card Unlock.”	
Reader Mode Locked	Reader Mode Locked	System	Generated when the reader mode has changed to “Locked.”	
Reader Mode Pin or Card	Reader Mode Pin or Card	System	Generated when the reader mode has changed to “Pin or Card” for the device.	
Reader Mode Unlocked	Reader Mode Unlocked	System	Generated when the reader mode has changed to “Unlocked.”	
Reader Module Firmware Upgraded	Reader Module Firmware Upgraded	System	Reader firmware has been updated.	
Reader Motor Stalled	Reader Motor Stalled	System	Generated when the motor stalls on a reader.	
Reader Motor Stalled Restored	Reader Motor Stalled Restored	System	Generated when a motor stalled condition has been restored.	

Alarm	Event	Event Type	Description	Duress*
Reader Reset	Reader Reset	System	Generated when the firmware resets the reader. This can happen if the reader is brand new or in the case of a failed/ incomplete download. Internal conditions, such as a possible corrupt memory, can also cause the firmware to reset. In these cases, the firmware will rewrite its entire storage with default values, overwriting the downloaded values. When this happens, the user must reprogram the lockset.	
Realtime Clock Updated	Realtime Clock Updated	System	The Real Time Clock (RTC) was updated.	
Register X Report	Register X Report	POS	Indicates a X report was generated. X reports are financial, end of day, clerk, etc. reports.	
Register Z Report	Register Z Report	POS	Indicates a Z report was generated. Z reports are the same as X reports, but resets totals to zero.	
Rejected Biometric Score	Rejected Biometric Score	Biometric	This event returns the rejected biometric score (the actual denied event is sent separately).	
Relay Contact Activated	Relay Contact Activated	System	Generated when a relay contact was activated.	
Relay Contact Deactivated	Relay Contact Deactivated	System	Generated when a relay contact was deactivated.	
Removed Object	Removed Object	Video	Generated when an object which was part of the background is detected as missing.	
Removed Object Restored	Removed Object Restored	Video	Generated when the object is returned to its original location or the background (after a certain time interval) is relearned.	

Alarm	Event	Event Type	Description	Duress*
Request to Exit - Door Used	Request to Exit - Door Used	System	Generated when the request to exit is granted and the door is used. **Note:** If the **Assumed Door Used** checkbox is selected on the Readers form, then the door is assumed to be used. This might interfere with this event.	
Request to Exit - Door Not Used	Request to Exit - Door Not Used	System	Generated when the request to exit is granted and the door is not used. **Note:** If the **Assumed Door Used** checkbox is selected on the Readers form, then the door is assumed to be used. This might interfere with this event.	
Retrieved	Retrieved	Intercom	Generated when a phone call is retrieved/ answered.	
Ringing	Ringing	Intercom	Generated when an intercom station/phone is ringing.	
Runaway Device	Runaway Device	System	Generated when the conditions specified for a runaway state are met. These conditions are configured on the System Options > Runaway Detection tab in System Administration.	
Runaway Device Restored	Runaway Device Restored	System	Generated when the conditions configured for runaway detection are no longer true.	

Alarm	Event	Event Type	Description	Duress*
Running Out of Disk Space	Running Out of Disk Space	NetDVMS	Generated when the live recording drive for the camera is running low on disk space. The criteria for generating this alarm is determined by the size of the drive and where the archive drive is located. For more information, refer to the NetDVMS documentation.	
Sales Subtotal	Sales Subtotal	POS	A transaction that reports the sale subtotal	
Schedule Change	Schedule Change	System	Generated when a schedule, added in the Scheduler, is changed.	
Schedule Executed	Schedule Executed	System	Generated when a schedule, added in the Scheduler, is executed.	
Scheduler Action Executed	Scheduler Action Executed	System	Generated when a scheduler action has executed.	
Scheduler Action Failed	Scheduler Action Failed	System	Generated when a scheduler action has failed.	
Security Alarm Acknowledge	Security Alarm Acknowledge	Fire	Generated when a security alarm has been acknowledged.	
Security Alarm Block Acknowledge	Security Alarm Block Acknowledge	Fire	Generated when all security alarms have been acknowledged at the fire panel.	
Security Alarm In	Security Alarm In	Fire	Generated when a new security alarm has been detected for the device.	
Security Alarm Out	Security Alarm Out	Fire	Generated when a device with a previous security alarm has returned to its normal state.	
Shorted Line Active	Shorted Line Alarm Active	System	Generated when a shorted line fault condition has been detected.	

Alarm	Event	Event Type	Description	Duress*
Shorted Line Restored	Canceled Shorted Line	System	Generated when a device with a shorted line fault condition has returned to its normal state.	
Signal Silence	Signal Silence	Fire	Generated when the alarm signal on the hardware has been silenced.	
Smart Card Authentication Failed	Smart Card Authentication Failed	System	Generated when a smart card authentication failed.	Yes
Smart VMD	Smart VMD	Video	Generated when a change is detected.	
Smart VMD Restored	Smart VMD Restored	Video	Generated 8 seconds after the last detection of a Smart VMD event.	
Status In	Status In	Fire	Generated when a status reporting device is active.	
Status - Missing Fire Supervision	Status - Missing Fire Supervision	Fire	Fire supervision is missing.	
Status Out	Status Out	Fire	Generated when a status reporting device has returned to the inactive state.	
Storage Failure	Storage Failure	Video	Indicates that something is wrong related to recording/retrieving video to/from hard drives. Includes LNVR database failure.	
Store Coupon	Store Coupon	POS	Indicates a store coupon.	
Supervisory Acknowledge	Supervisory Acknowledge	Fire	Generated when a supervisory condition has been acknowledged.	
Supervisory Block Acknowledge	Supervisory Block Acknowledge	Fire	Generated when all supervisory conditions have been acknowledged at the fire panel.	
Supervisory In	Supervisory In	Fire	Generated when a new supervisory condition has been detected for the device.	

Alarm	Event	Event Type	Description	Duress*
Supervisory Out	Supervisory Out	Fire	Generated when a device with a previous supervisory condition has returned to its normal state.	
System Reset	System Reset	Fire	Generated when the fire panel has been reset.	
Tax Amount	Tax Amount	POS	Event that indicates the tax amount.	
Taxable Subtotal	Taxable Subtotal	POS	Transaction that reports the taxable subtotal	
Timeout Exceeded - No Second Card	Timeout Exceeded - No Second Card	Area Control	Generated when no second card was presented within the time limit for the area/reader using two-man control.	Yes
Time Out-Of-Sync	Time Out-Of-Sync	Video	Generated when the time stamp feature is enabled and the time on the camera has a difference of 20 seconds or more from the video recorder time.	
Time Out-Of-Sync Restored	Time Out-Of-Sync Restored	Video	Generated when the time difference between the camera and video recorder returns to less than 20 seconds.	
Total Amount Due	Total Amount Due	POS	Transaction indicating the total amount due.	
Transaction Number	Transaction Number	POS	Event Generated that indicates the transaction number of the sales transaction.	
Transfer, Diagnostics	Transfer, Diagnostics	System	Generated when a user is connected to the device for diagnostic purposes.	
Transfer, History	Transfer, History	System	Generated when a history data was transferred from the device to the parent device.	

Alarm	Event	Event Type	Description	Duress*
Transfer, PDA To Lock	Transfer, PDA To Lock	System	Generated when the device (lockset) is programmed/ reprogrammed through a download from a Mobile Configurator.	
Transferred Call		Intercom	Generated if an intercom call is transferred.	
Transmitter Alarm	Transmitter Alarm	Transmitter	Generated when the button or input on a transmitter has been activated.	
Transmitter Alarm Restored	Transmitter Alarm Restored	Transmitter	Generated when the transmitter alarm has been restored.	
Transmitter Inactivity	Transmitter Inactivity	Transmitter	Transmitter has been inactive longer than the supervision interval	
Transmitter Low Battery	Transmitter Low Battery	Transmitter	Transmitter low battery alarm	
Transmitter Low Battery Restored	Transmitter Low Battery Restored	Transmitter	Generated when a transmitter low battery has been restored.	
Transmitter Pre-Tilt	Transmitter Pre-Tilt	Transmitter	Generated when the transmitter is in the pre-tilt state.	
Transmitter Pre-Tilt Restored	Transmitter Pre-Tilt Restored	Transmitter	Generated when the transmitter has returned to normal from the pre-tilt state.	
Transmitter Pull Cord Alarm	Transmitter Pull Cord Alarm	Transmitter	Generated when the pull cord on a transmitter has been pulled and is in alarm.	
Transmitter Pull Cord Restored	Transmitter Pull Cord Restored	Transmitter	Generated when the transmitter pull cord alarm has been restored.	
Transmitter Tamper	Transmitter Tamper	Transmitter	Transmitter tamper alarm.	
Transmitter Tamper Restored	Transmitter Tamper Restored	Transmitter	Generated when a transmitter tamper has been restored.	
Transmitter Temporary Tilt Disable	Transmitter Temporary Tilt Disable	Transmitter	Generated when the transmitter temporary tilt has been disabled.	

Alarm	Event	Event Type	Description	Duress*
Transmitter Tilt	Transmitter Tilt	Transmitter	Generated when a tilt condition on the transmitter has been detected.	
Transmitter Tilt Disabled	Transmitter Tilt Disabled	Transmitter	Generated when the transmitter tilt function has been disabled.	
Transmitter Tilt Enabled	Transmitter Tilt Enabled	Transmitter	Generated when the transmitter tilt function has been enabled.	
Transmitter Tilt Restored	Transmitter Tilt Restored	Transmitter	Generated when the tilt condition on the transmitter has been restored.	
Transmitter Acknowledge	Transmitter Acknowledge	Transmitter	This event is reported when an alarm generated by a transmitter has been acknowledged.	
Transmitter No Response	Transmitter No Response	Transmitter	This event is reported when an alarm generated by a transmitter has not been acknowledged.	
Transmitter Touch Alarm	Transmitter Touch Alarm	Transmitter	Alarm generated by a transmitter when the item it is protecting is touched.	
Transmitter Removal Alarm	Transmitter Removal Alarm	Transmitter	Alarm generated by a transmitter when an item it is protecting is removed.	
Trouble Acknowledge	Trouble Acknowledge	Fire	Generated when the trouble condition has been acknowledged.	
Trouble Acknowledge Clear	Trouble Acknowledge Clear	Fire	Generated when a trouble condition that has been cleared from the system has been acknowledged by a user.	
Trouble Bell #	Trouble Bell 1 or 2	Relay/ Sounder	Generated when Trouble bell 1 or 2 is in alarm.	
Trouble Bell # Restore	Trouble Bell 1 or 2 Restore	Relay/ Sounder	Generated when Trouble bell 1 or 2 is restored.	
Trouble Block Acknowledge	Trouble Block Acknowledge	Fire	Generated when all trouble conditions have been acknowledged at the fire panel.	

Alarm	Event	Event Type	Description	Duress*
Trouble In	Trouble In	Fire	Generated when a new trouble condition has been detected for the device.	
Trouble Out	Trouble Out	Fire	Generated when a device with a previous trouble condition has returned to its normal state.	
Unanswered Call	Unanswered Call	Intercom	Generated if a ringing intercom call goes unanswered.	
Unexpected Access	Unexpected Access	System	Generated when a user successfully exits using an unexpected exit reader, after gaining access to a specific entry reader, and the “must proceed to exit readers” option is enabled.	
Unexpected Access Attempt	Unexpected Access Attempt	System	Generated when a user attempts to exit using an unexpected exit reader, after gaining access to a specific entry reader, and the “must proceed to exit readers” option is enabled.	
Unknown Elevator Terminal	Unknown Elevator Terminal	System	Generated when an elevator terminal is detected that has not been configured in the system.	
Unknown User Command	Unknown User Command	System	Generated when an unknown user command is entered through a reader. For example, if a cardholder enters the command *1234# (where that command means nothing) an unknown user command alarm is sent to Alarm Monitoring. The numbers entered as the command are used as the event text for the alarm.	
Unlocked Under AFC	Unlocked Under AFC	System	Lock has entered AFC state.	

Alarm	Event	Event Type	Description	Duress*
Unlocked Mode Change Denied: Blocked Mode	Unlocked Mode Change Denied: Blocked Mode	System	Automatic scheduled change to unlocked mode was denied because lock is in blocked mode.	
Unlocked Mode Change Denied: Low Battery	Unlocked Mode Change Denied: Low Battery	System	Automatic scheduled change to unlocked mode was denied due to low battery condition.	
Unlocked Mode Change Denied: Secured Mode	Unlocked Mode Change Denied: Secured Mode	System	Automatic scheduled change to unlocked mode was denied because lock is in secured mode.	
Unlocked Under First Card Unlock	Unlocked Under First Card Unlock	System	First card unlock mode; door is unlocked.	
Unsupported Hardware	Unsupported Hardware	System	Generated when hardware that is not supported is added to the system.	
Untyped Abort	Untyped Abort	Trouble	Generated when an alarm for a device of an unknown type has been aborted/canceled.	
Untyped Alarm	Untyped Alarm	Trouble	Generated when an alarm for a device of unknown type occurs.	
Untyped Alarm Restore	Untyped Alarm Restore	Trouble	Generated when the device of an unknown type is restored.	
Untyped Bypass	Untyped Bypass	Trouble	Generated when a device of an unknown type has been bypassed.	
Update: Now able to Achieve Current Required Storage Setting	Update: Now able to Achieve Current Required Storage Setting	System	Generated by an LNVR recorder when the recording rate drops to allow the video storage to be full in the same or more number of days than defined by the user.	
Use Limit Exceeded	Use Limit Exceeded	Denied	Access was denied because the use limit for the badge has been exceeded.	Yes

Alarm	Event	Event Type	Description	Duress*
User Failed to Reach Destination	User Failed to Reach Destination	System	Generated when a user fails to exit at a specific exit reader, after gaining access to a specific entry reader, before the timeout value expires.	
User Generated Video Event	User Generated Video Event	Video	Video events are typically created automatically by the system based on an event from an external device. This allows the user to generate an event that is not tied to any device. It can be created from any camera with any user defined time limit from within the video player window in Alarm Monitoring. This event can then be included in reports, or have a trace performed like any other event in the system.	
Value Added	Value Added	POS	Event that indicates value added.	
Video Event Threshold Reached	Video Event Threshold Reached	Video	Generated when the user-defined event threshold has been reached and exceeded. (The percent of disk space used by video events has been reached, typically signaling the archive server to start archiving or purging.)	
Video Failover Failed	Video Failover Failed	Video	Generated when the camera is configured for failover and failover cannot be activated on this camera.	

Alarm	Event	Event Type	Description	Duress*
Video Failover Restored	Video Failover Restored	Video	Generated when the camera is configured for failover and secondary recorder is currently recording video from the camera and secondary recorder determined that the primary recorder came back online and started recording video from the camera. Secondary recorder will stop recording video from the camera. Alarm Monitoring users should log off of the application and back on when the primary recorder comes back online.	
Video Failover Started	Video Failover Started	Video	Generated when the camera is configured for failover and secondary recorder determined that the primary recorder is not recording video from the camera, so secondary recorder starts recording from this camera. Alarm Monitoring users should log off of the application and back on when failover occurs.	
Video Graininess Restored	N/A	N/A	Displayed after noise (graininess) in the video has been reduced.	
Video Overflow Restored	Video Overflow Restored	Video	Generated when the recorder is no longer having troubles handling incoming video.	
Video Overflow Started	Video Overflow Started	Video	Generated when the recorder determined that it cannot handle incoming video. Usually it happens when hard drive or CPU utilization is close to 100%, so recorder cannot keep up with amount of video.	

Alarm	Event	Event Type	Description	Duress*
Video Server Disk Full	Video Server Disk Full	Video	Generated when the user-defined event threshold has been exceeded by 5% or more. (The percent of disk space used by video events has been exceeded by at least 5%, typically signaling the archive server to start archiving or purging.) If a user-defined event threshold has not been defined, this alarm/event will be generated when the video server disk space is 75% full of video events.	
Video Server is Not Recording	Video Server is Not Recording	Video	Generated when it has been detected that the video recorder is no longer recording. A check is done periodically (default is every 10 minutes) to check to make sure that video is still being recorded. This event is generated when the check fails.	
Video Source Signal Lost	Video Source Signal Lost	Video	Generated when the video signal from a channel is lost from the video server. This alarm may be accompanied by a Communications Lost alarm.	
Video Source Signal Restored	Video Source Signal Restored	Video	Generated when the video signal from a channel is restored to the video server. This alarm maybe accompanied by a Communications Restored alarm.	
Video Storage Unavailable	Video Storage Unavailable	Video	Generated when the recorder cannot record video to a drive.	
Void or Error Correction	Void or Error Correction	POS	Transaction that indicates a void or error correction	

Alarm	Event	Event Type	Description	Duress*
Walk Test ##	Walk Test ##	Fire	Generated when walk test ## is initiated. A walk test is used to test devices in the system and report devices addressed incorrectly. The device and the first zone programmed for this device are reported with each message.	
Walk Test Uninstalled	Walk Test Uninstalled	Fire	Generated when the reported device was part of a walk test and has been physically disconnected from the system.	
Walk Test Unprogrammed	Walk Test Unprogrammed	Fire	Generated when the reported device was part of a walk test and has been removed from the system (it is not longer configured in the system).	
Walk Test Untest	Walk Test Untest	Fire	Generated when the reported device is no longer being tested (part of a walk test).	
Warning: Unable to Achieve Current Required Storage Setting	Warning: Unable to Achieve Current Required Storage Setting	System	Generated by an LNVR recorder when video storage will be full in less number of days than defined by the user.	
Warning: Unable to Meet Required Storage Setting! Deleting Oldest Video	Warning: Unable to Meet Required Storage Setting! Deleting Oldest Video	System	Generated by an LNVR recorder when there is no space available to record to, so the oldest file will be deleted in order to continue recording.	
Warning: Poor Visibility	N/A	N/A	This warning appears when the camera's view of a scene is impaired by glare, fog, etc. The sensitivity of the Poor Visibility warning can be adjusted in the Channel Configuration dialog.	

Alarm	Event	Event Type	Description	Duress*
Warning: Video Graininess	N/A	N/A	This warning appears when the video is noisy (grainy.) The alarm may also be generated in scenes with very fine detail, such as heavy vegetation.	
Wireless Smoke Detector	Wireless Smoke Detector	Fire	A wireless smoke detector has generated an alarm.	
WLM Firmware Upgraded	WLM Firmware Upgraded	System	Radio module firmware was updated	

* The duress column marks which alarm events can be used as duress events if your system is configured for duress.

NGP Alarm/Event Descriptions

Alarm	Event	Event Type	Description
All Lockouts Removed	All Lockouts Removed	System	
Area Alarm - Confirmed	Area Alarm - Confirmed	Area Control	Applies to panels configured in the UK (APCO). A confirmed alarm is when two independent inputs become active in a armed area within the configured timeout.
Area Alarm - Unconfirmed	Area Alarm - Unconfirmed	Area Control	Applies to panels configured in the UK (APCO). An unconfirmed alarm is when one input becomes active in a armed area.
Area APB Reset	Area APB Reset	System	
Area Arm Failure	Area Arm Failure	System	When the arming of an area fails.
Area Arm with Override	Area Arm with Override	System	Generated when a user with Master Override permission in the assigned permission profile arms an area.
Area Confirm Alarm Reset	Area Confirm Alarm Reset	System	Applies to panels configured in the UK (APCO).Generated when a Confirmed alarm is reset at the panel. This is accomplished by logging in with the service account, then with a valid user account and then resetting the confirmed alarm.
Area Limit Minimum	Area Limit Minimum	Area Control	
Armed Off	Armed Off	System	Arming has been turned OFF for the indicated Area (Disarmed).
Armed On	Armed On	System	Arming has been turned ON for the indicated Area (Full Armed).

Alarm	Event	Event Type	Description
Armed On with Bypasses	Armed On with Bypasses	System	Generated when an area is armed while a point is bypassed.
Armed on with Isolates	Armed on with Isolates	System	Generated when an area is armed while an input has been isolated.
Backup Battery Critical	Backup Battery Critical	System	The panel backup battery has reached the cutoff voltage defined in the panel configuration. A panel shutdown will occur.
Backup Battery Low	Backup Battery Low	System	The panels backup battery is has reached the low voltage defined in the panel configuration.
Bad Card Lockout	Bad Card Lockout	System	Generated when a invalid badge is presented to a reader over the “Invalid access/Individual lockout/Number of invalid card” threshold.
Bad PIN Lockout	Bad PIN Lockout	System	This occurs if a keypad user exceeds the threshold of incorrect PIN entries at the keypad.
Bad System ID	Bad System ID	System	
Battery Restored	Battery Restored	System	
Battery Trouble	Battery Trouble	System	
Cannot Arm - Users Left In Area	Cannot Arm - Users Left In Area	System	
Central Station Report Delay	Central Station Report Delay	System	The panel has exhausted its attempts to report alarms to central station and will stop sending alarms for a pre-defined time interval. The length of time the panel will wait before making further attempts to transmit alarms to central station depends on the SIA/CID > Communication > Call Sequence setting.
Central Station Report Success	Central Station Report Success	System	

Alarm	Event	Event Type	Description
Command Point Failure	Command Point Failure	System	
Command Point Reset	Command Point Reset	System	
Command Point Trip	Command Point Trip	System	
Config No Reply	Config No Reply	System	
Denied - Area Out of Schedule	Denied - Area Out of Schedule	Access Denied	The cardholder does not have permission to access this reader's area outside of its arming schedule.
Denied - Dual Custody Violation	Denied - Dual Custody Violation	Access Denied	This reader cannot be accessed by a single presented card.
Denied - Group Mismatch	Denied - Group Mismatch	Access Denied	
Denied - No Off Authority	Denied - No Off Authority	Access Denied	Event generated when cardholder swipes badge at a door in an unarmed area and doesn't have “Enter area when disarmed” permission profile permission.
Denied - No On Authority	Denied - No On Authority	Access Denied	Event generated when cardholder swipes badge at a door in an armed area and doesn't have “Enter area when Armed” permission profile permission.
Denied - No Stay Authority	Denied - No Stay Authority	Access Denied	Event generated when cardholder swipes badge at a door in an armed-stay area and doesn't have “Enter area when Armed-stay” permission profile permission.
Denied - Pending Enroll	Denied - Pending Enroll	Access Denied	
Denied, duplicate card	Denied, duplicate card	System	
Denied, duplicate card	Denied, duplicate card	Access Denied	

Alarm	Event	Event Type	Description
Door Held Open Pre Alarm	Door Held Open Pre Alarm	System	This door will report a 'Door Held Open' alarm at the end of the configured pre-alarm time. The event generated when the Door held open pre-alarm timer has expired.
Door Locked Out	Door Locked Out	System	
Door Mag Trouble Clear	Door Mag Trouble Clear	System	
Door MagTrouble	Door MagTrouble	System	
Door Reinstated	Door Reinstated	System	The reader(s) on this door have been returned to their previous reader access mode (used with Door Locked/Door Unlocked)
Door Restore	Door Restore	System	
Dual Custody User Off (Disarm)	Dual Custody User Off (Disarm)	System	The indicated area that requires 'Dual Custody' has been disarmed.
Emergency Off	Emergency Off	System	The area is armed by schedule, and someone with “emergency disarm” privileges is disarming it.
Entry Exit	Entry Exit	System	I have never seen this alarm
Fap Processing Start	Fap Processing Start	System	A triggered input for the area has started 'False Alarm Prevention' processing Event is generated when the first FAP point in a armed area goes active.
Grant Last User (Override)	Grant Last User (Override)	Access Granted	
Granted-Dual Custody	Granted-Dual Custody	Access Granted	A reader requiring 'Dual Custody' has granted access.
Granted-Escort	Granted-Escort	Access Granted	A reader requiring 'Escort' has granted access.

Alarm	Event	Event Type	Description
Granted-Exit-Dual Custody	Granted-Exit-Dual Custody	Access Granted	An exit reader (entering outside area) requiring 'Dual Custody' has granted access.
Granted-Exit-Escort	Granted-Exit-Escort	Access Granted	Cardholder has permission profile with “Escort” configured is granted access to a door that goes to the “outside” area.
Granted-Exit-Master	Granted-Exit-Master	Access Granted	Card holder has permission profile with “Master Override” enabled swipes card at “outside” reader.
Granted-Master	Granted-Master	Access Granted	Card holder has permission profile with “Master Override” enabled swipes card at reader other than “outside” reader.
Granted-Pending Entry	Granted-Pending Entry	Access Granted	Event generated when valid badge is swiped at the reader and the door has not been opened when door is NOT configured for “Assume door used”.
HSC Reset	HSC Reset	System	
HSC-IP Trouble	HSC-IP Trouble	System	
HSC-IP Restored	HSC-IP Restored	System	
Isolate	Isolate	System	Event generated when a point is Disabled.
Memory Backup Battery Low	Memory Backup Battery Low	System	
No Escort Authority	No Escort Authority	Access Denied	Reader event generated when a badge that requires an escort is followed with a badge swipe that doesn't have Escort permissions.

Alarm	Event	Event Type	Description
No Intrusion Off or Stay Authority	No Intrusion Off or Stay Authority	Access Denied	Event generated when Card swiped at Armed area reader does not have permission profile with “Enter area while Off” AND “Enter area while Armed-stay”.
Output Error	Output Error	System	
Panel Reboot to Factory Defaults	Panel Reboot to Factory Defaults	System	
Panel Reset Watchdog	Panel Reset Watchdog	System	
Panel Restart Due to Power Failure	Panel Restart Due to Power Failure	System	Event generated when a panel without battery backup looses power.
Pending first user	Pending first user	System	
POD Trouble	POD Trouble	System	Generated when an alarm loses communication with a POD. The POD will be offline during this condition. PODs are external modules connected via RS-485.
Point Test Fail	Point Test Fail	System	
Reader Authority Toggle	Reader Authority Toggle	Access Denied	
Reader in Dual Custody Mode	Reader in Dual Custody Mode	System	
Reader in Escort Mode	Reader in Escort Mode	System	
Reader Mode PIN Only	Reader Mode PIN Only	System	
Reader in Normal Mode	Reader in Normal Mode	System	
Reader Toggle	Reader Toggle	Access Denied	
Schedule Resumed	Schedule Resumed	System	Generated when a area arming schedule has been resumed.
Schedule Suspend	Schedule Suspend	System	

Alarm	Event	Event Type	Description
SIA Session Code	SIA Session Code	System	
Supply Fuse Restored	Supply Fuse Restored	System	
Supply Fuse Trouble	Supply Fuse Trouble	System	
System APB reset	System APB reset	System	
System Confirm	System Confirm	System	Applies to panels configured in the UK (APCO). The system will produce this alarm if a Confirmed Area Alarm is generated.
System Confirm Alarm Reset	System Confirm Alarm Reset	System	Applies to panels configured in the UK (APCO).Generated when a Confirmed alarm is reset at the panel. This is accomplished by logging in with the service account, then with a valid user account and then resetting the confirmed alarm.
System Message	System Message	System	
System Password Fail	System Password Fail	System	This event cannot be generated at this time.
System Program Changed	System Program Changed	System	
System Program Fail	System Program Fail	System	
System Restored	System Restored	System	
System Trouble	System Trouble	System	
System Unconfirm	System Unconfirm	System	
Telco SIA/CID) Reset	Telco SIA/CID) Reset	System	The panel will now resume attempts to report alarms to central station. This alarm is reported if prior attempts to report events to central station failed.
Unauthorized Off	Unauthorized Off	System	
Upload Okay	Upload Okay	System	

Alarm	Event	Event Type	Description
USB 1 Fuse Blown	USB 1 Fuse Blown	System	
USB 1 Fuse Reset	USB 1 Fuse Reset	System	
USB 2 Fuse Blown	USB 2 Fuse Blown	System	
USB 2 Fuse Reset	USB 2 Fuse Reset	System	
User APB Reset	User APB Reset	System	
Verify User	Verify User	System	
Wandering Patient Alarm Reset	Wandering Patient Alarm Reset	System	
Wandering Patient at Door	Wandering Patient at Door	System	
Warning - Users Left In Area	Warning - Users Left In Area	System	

APPENDIX C

Multimedia Capture

Multimedia Capture contains forms with which you can:

- Capture a cardholder or visitor's photo
- Import an existing photo
- Optimize photo image quality
- Record a cardholder's signature
- Capture and define cardholder biometric templates

Multimedia Capture contains up to nine forms: the Photo form, the Signature form, the Hand Geometry form, the Fingerprint (Bioscrypt) form, the OpenCapture form, the Iris (IrisAccess 3000) form, and the Iris (IrisAccess iCAM) form.

In the System Administration, Alarm Monitoring, ID CredentialCenter, and Visitor Management applications, Multimedia Capture is opened by selecting the [Capture] button when adding or modifying a record in the Cardholders folder.

Required Licenses and Permissions

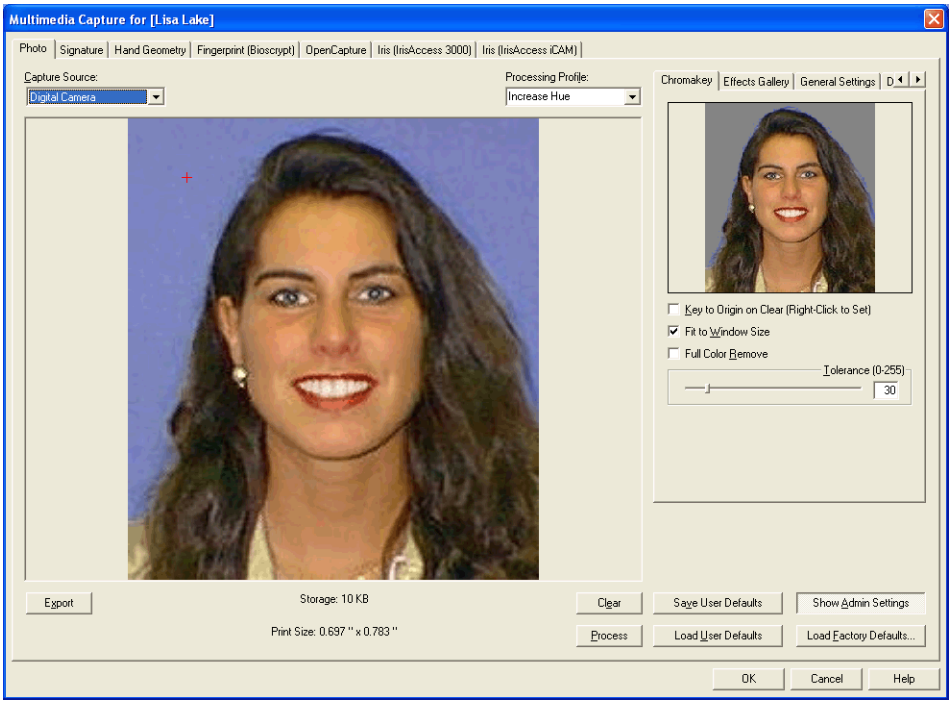
The availability of certain features in Multimedia Capture are subject to licensing restrictions. A user's permissions must also be set on the Cardholder Permission Groups form in the Users folder. For more information, refer to Cardholder Permission Groups Form on page 364.

Multimedia Capture feature	Required license	Required Cardholder Level capture permission
Image Processing window	Image Capture (STD)	Image Processing
WDM Video capture source	Image Capture (STD)	Photo
FlashPoint/MCI Video capture source	Image Capture (STD)	Photo

Multimedia Capture feature	Required license	Required Cardholder Level capture permission
WDM Video Settings, FlashPoint/MCI Video Settings and FlashPoint/MCI Video I/O Settings sub-tabs	Image Capture (STD)	Photo and Advanced
Scanner & Digital Camera capture sources	Image Capture (STD)	Scanner
Scanner & Digital Camera Settings sub-tabs	Image Capture (STD)	Scanner and Advanced
Signature capture source	Image Capture (STD)	Signature
Signature Settings sub-tab	Image Capture (STD)	Signature and Advanced
Hand Geometry form	HandKey Hand Geometry Hardware Support (SWG-1400)	Biometrics
Fingerprint (Bioscrypt) Form	Bioscrypt Veri-Series Hardware Support (SWG-1402)	Biometrics
OpenCapture Form	OpenCapture Recognition Hardware Support (Cross Match ID 500, Cross Match Verifier 300, and Sagem Morpho Smart Optical scanners)	Biometrics
Iris (IrisAccess 3000) Form	IrisAccess Application Support (SWG-LGxxx)	Biometrics
Iris (IrisAccess iCAM) Form	IrisAccess Application Support (SWG-LGxxx)	Biometrics

Photo Form

The Photo form is used for capturing cardholder's images. Photos can be captured via file import (bitmapped and/or vector), or via cameras or scanners (bitmapped).



Capture Source

Select the type of information you want to capture. Choices include:

- WDM Video - the cardholder's photo is captured from live video. When you select the WDM Video capture source, the WDM Video Settings sub-tab becomes available.
- Flashpoint/MCI Video - the cardholder's photo is captured from live video. When you select the FlashPoint/MCI Video capture source, the FlashPoint/MCI Video Settings sub-tab becomes available.
- Signature - the cardholder enters his or her signature using a signature capture tablet and stylus. (This option is only available when Signature form is selected.)
- Scanner - a scanner device creates a computer image file from an existing hardcopy photo. When you select the Scanner capture source, the Scanner Settings sub-tab becomes available.
- Digital Camera - a digital camera is attached to the computer so that images stored in the camera can be transferred to the system. When you select the Digital Camera capture source, the Digital Camera Settings sub-tab becomes available.
- File Import - an existing computer image file is added to the system.

Processing Profile

Select an effect profile for the selected image. Effect profiles are defined in the Image Processing window. Click [Process] to open the Image Processing window. They system is configured with a set of default image processing profiles that can be applied.

Multimedia window

Depending on your selection from the **Capture Source** drop-down list, this window displays either live video, signature input, scanner input, a digital camera image or an imported file.

Export

Click this button to save the current captured image as an image file on a disk. Minimal compression will be used so that the image is stored in the best possible quality. The crop window will be used when exporting if an image is bitmapped. The following default filename and extensions apply when exporting:

When the Photo form is selected:

- If the photo is bitmapped and the crop window is in use, the portion of the image within the crop window will be saved. Otherwise, the whole photo will be saved.
- If the current record has no name assigned to the cardholder, the filename default is "no_name Photo." Otherwise, the filename will default to the cardholder's name.

When the Signature form is selected:

- If the signature is bitmapped and the crop window is in use, the portion of the signature within the crop window will be saved. Otherwise, the whole signature will be saved.
- If the record has no cardholder name, the filename default is "no_name Sig" plus the filename extension. Otherwise, it defaults to the cardholder name plus the filename extension.

When the Graphic form is selected:

- If the graphic is bitmapped and the crop window is in use, the portion of the graphic within the crop window will be saved. Otherwise, the whole graphic will be saved.
- If the graphic is a new one being imported into the database, the filename default is "New Layout Graphic" plus the filename extension. Otherwise, it defaults to the graphic name plus the file extension.

Freeze

Select this button to freeze the live video in order to capture a cardholder's photo. This button is displayed only when either "WDM Video" or "FlashPoint/MCI Video" is selected from the **Capture Source** drop-down list.

Unfreeze

Select this button to resume live video. This button is displayed only when either "WDM Video" or "FlashPoint/MCI Video" is selected from the **Capture Source** drop-down list.

Open

Click this button to display an Open window from where you can select a drive, directory and filename to import an existing photo. This button is displayed only when "File Import" is selected from the **Capture Source** drop-down list.

Clear

Click this button to clear the contents of the multimedia window. This button is displayed only when "Signature," "Scanner," "Digital Camera", or "File Import" is selected from the **Capture Source** drop-down list.

Sign

Click this button to activate the signature pad so that the cardholder can enter his or her signature. This button is displayed only when "Signature" is selected from the **Capture Source** drop-down list.

Stop

Click this button to notify the system that the cardholder has finished entering his or her signature and deactivate the signature pad. This button is displayed only when "Signature" is selected from the **Capture Source** drop-down list.

Preview
Click this button to activate the scanner, so that the existing image can be digitized (scanned) into the system. This button is displayed only when “Scanner” is selected from the **Capture Source** drop-down list.

Scan
Click this button to activate the scanner, so that the existing image can be digitized (scanned) into the system. This button is displayed only when “Scanner” is selected from the **Capture Source** drop-down list.

Process
Click this button to open the Image Processing window from where you can manipulate the captured photo to improve its quality.

Save User Defaults
Click this button to save the current settings as the default settings on this workstation. The settings will be applied to all Multimedia Capture forms and sub-tabs; however, they do not include the set of image processing profiles, which are maintained separately by the Image Processing window.

Show Admin Settings
Select this button to view all the forms and sub-tabs applicable to the current capture source. When not selected, only the Chromakey and Effects Gallery sub-tabs will be displayed.

Load User Defaults
Click this button to display the previously saved (default) settings for this workstation. The settings will be applied to all Multimedia Capture forms and sub-tabs.

Load Factory Defaults
Click this button to open the Load Factory Defaults window where you can reset the capture settings back to the default values for your specific capture hardware.

OK
Saves your changes and closes Multimedia Capture.

Cancel
Closes the window and returns you to the Cardholder, Badge or Access Levels form. Does not save any changes made in Multimedia Capture.

Help
Displays online assistance for Multimedia Capture.

General Capture Procedures

The following procedures can be used on this form.

Open Multimedia Capture

Multimedia Capture opens when you click [Capture] while adding or modifying a record in the Cardholders folder.

1. In Alarm Monitoring, select ***Badge Info*** from the ***View*** menu. In all other applications, select ***Cardholders*** from the ***Administration*** menu. The Cardholders folder opens.
2. Display a cardholder record. To do this, you can either add a cardholder record or search for an existing record. For more information, refer to Add a Cardholder Record on page 103 or Search for a Cardholder Record on page 88.
3. Click [Modify]. (Although you can see both cardholders and visitors in Visitor Management, the [Modify] button is only active for visitors.)
4. Click [Capture]. Multimedia Capture opens.

Load (User or Factory) Default Settings

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Photo, Signature, or Graphic tab.
3. Click [Load Factory Defaults] or [Load User Defaults].
4. If you are loading user defaults, the settings automatically populate.
5. If you are loading factory default settings, the Load Factory Defaults dialog opens.
   a. Select the profile for the hardware capture device.

Note: The difference between high resolution and low resolution digital camera profiles is that they have different default crop window sizes.

   b. Click [OK].

Export an Image

OnGuard exports the most recently saved image. Even if you are displaying live video or recording a signature at the time you initiate export, OnGuard exports the last image saved. If the image is cropped, only the cropped portion is exported.

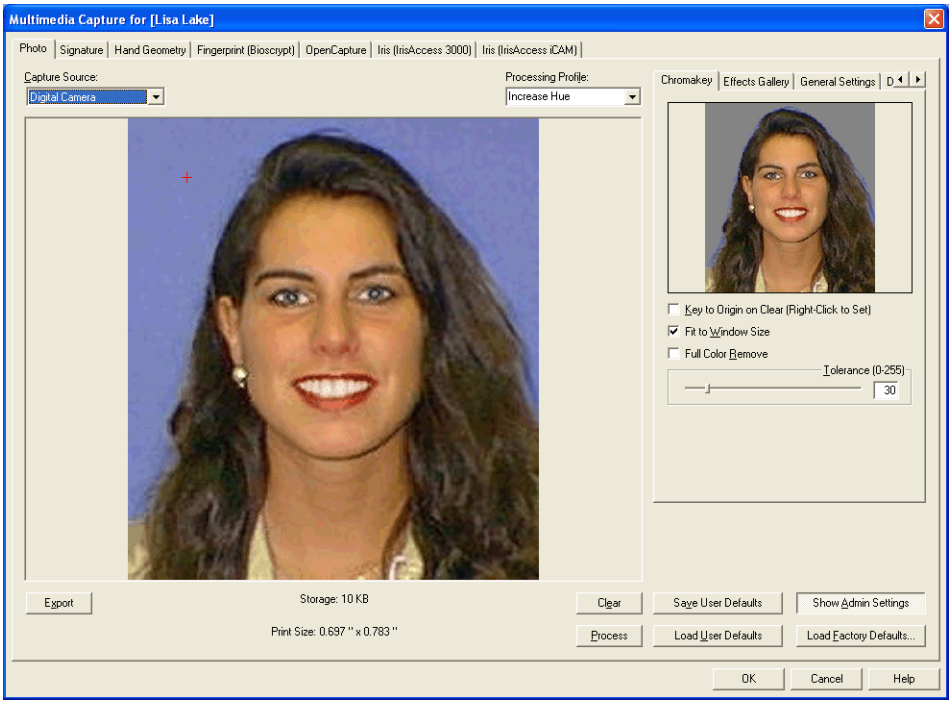
1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Photo, Signature or Graphic tab.
3. Display the image and click [Export].
4. Depending on how the system is configured, the Save As window opens. Enter the filename and click [Save]. Otherwise, the file is automatically named and exported to the default directory set up in the Multimedia Capture admin settings (File I/O Settings sub-tab).

Formats Exported

OnGuard exports images in the following formats:

- JPG format if the image is bitmapped and has more than 256 colors.
- PNG format if the image is bitmapped and has 256 colors or less.
- EMF format if the image is vector.

Chromakey Sub-tab



The Chromakey sub-tab allows you to control if and how the system determines background transparency information for bitmapped images. Chromakey does not apply to non-bitmapped (vector) images.

A typical application of chromakey is to capture cardholder/visitor images using a solid color backdrop. Then, apply chromakey to the images (remove the background color) and print the badge. The cardholder/visitor's image displays over the background image.

Chromakey output

Displays the image with the current Chromakey settings applied. When printing a badge, you may want to first preview the badge and zoom in to enlarge the display, to make sure that your Chromakey settings produced the desirable result.

Key to Origin on Clear (Right-Click to Set)

Controls the position of the key (red cross-hairs) upon loading of a new image. The key position is selected using the mouse to right-click over the image. When this check box is selected, when the current image is cleared, the key position is reset to the origin (at the top left corner of the crop window). When this check box is not selected, when the current image is cleared, the key position is preserved.

Fit to Window Size

When this check box is selected, the current image is scaled to fit within the available viewing area. Depending on the size of the image, it will be reduced or enlarged to fit the window.

Full Color Remove

When this check box is selected, the chromakey feature will determine which pixels are background pixels strictly by color matching alone. Every pixel of the image is compared against the key color, from left-to-right, top-to-bottom. Each pixel that differs from the key color is determined to be a background pixel. The tolerance setting determines how much the colors have to differ from the key color to be considered as background. When this check box is not selected, the chromakey feature will determine which pixels are background pixels in the same manner as a drawing program's flood-fill feature. The filling starts at the origin and spreads outward, stopping at parts of the image that differ from the key color. The tolerance setting determines how much the colors have to differ to stop the fill.

Full color remove works well with graphic images but not with photos when the color of the person's eyes or clothing is very similar to the background color.

Tolerance (0-255)

Determines how much deviation from the exact chromakey color match is tolerable. Choose a value in the range of 0-100. The higher the tolerance value the more colors that will be chromakeyed out (the more colors that will be converted to background).

Chromakey Sub-tab Procedures

The following procedures can be performed on this form.

Apply Chromakey to an Image

Note: Chromakey is available only when the captured image is bitmapped.

1. Open Multimedia Capture and display an image. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo or Graphic tab, click the Chromakey sub-tab.
3. In the main window, identify the color you want to make transparent by right-clicking the mouse over the original image (and inside the crop window if there is one). When you right-click, a red cross hair displays or repositions itself. The red cross hair identifies the color the chromakey tolerance value applies to.

4. On the Chromakey sub-tab:
   a. Select the **Fit to Window** Size check box if you want to view the entire image in the Chromakey window.
   b. Select the **Full color Remove** check box to remove the selected color from the entire screen. This feature works well with graphic images but not photos where the person's eye color may match the background you are trying to remove.
   c. Use the **Tolerance** slider to control the depth of the chromakey effect. The Chromakey window displays the changes.
   d. Use the **Key to Origin on Clear (Right-Click to Set)** check box to reset the cross hair position to the top left corner of the image when you click [Clear].
5. Click [OK].

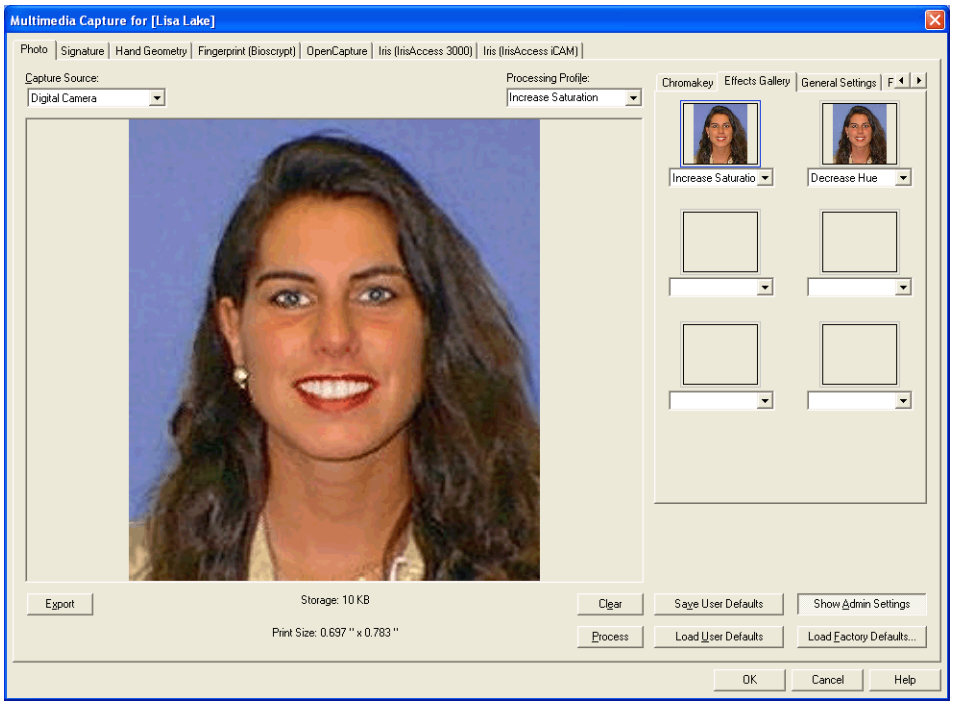
Chromakey Tips

The following characteristics produce the best chromakey results:

- High quality images
- Deep blue or green (highly saturated) backgrounds (light gray and white do not work well)
- Uniform background lighting
- No shadows
- Background color significantly different than the subject's eye and clothing color

Effects Gallery Sub-tab

The Effects Gallery displays up to six pre-defined effect profiles. Choices include: increase or decrease hue, increase or decrease saturation, increase or decrease contrast, and sharpen. An *effect profile* contains special effects that can be applied to bitmapped images only.



You can also customize an effect profile. When you customize an effect profile you can choose from 21 different effects. Furthermore, many of these effects have settings that allow you to increase or decrease the intensity of that effect. Multiple effects can be combined to achieve the desired result. For more information, refer to Create an Effect Profile on page 1352.

Use the Effects Gallery

1. Open Multimedia Capture and display an image. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo or Graphic tab, click the Effects Gallery sub-tab.
3. Select an effect profile from the drop-down list.
4. To apply the effect on the currently displayed image, select the thumbnail image such that a blue line encompasses the perimeter of the thumbnail.

Image Processing Window

Preview boxes

Any of the six boxes each containing a thumbnail of the captured image with an effect profile applied.

Effect profile

Choices in these drop-down lists (located below the six thumbnails of the captured image) include the names of all currently defined effect profiles. Select a profile to be applied to each thumbnail.

Image Processing Window

Original Image

Displays a miniature view of an original (unprocessed) captured image.

Processed Image

Displays a miniature view of an image with an effect profile applied. This enables you to preview the outcome of combined image effects.

Effect Library

Lists the available effects you can apply to the captured image. Choices include:

- None - applies no effects to the image.
- Intensity - increases or decreases the overall intensity level of the light in the image. Adjust the brighter areas by making them brighter or darker. You can choose a value in the range of -100% to +100%. Negative values make the image darker; positive values lighten the image.
- Contrast - increases or decreases the range of gray levels contained in the image, adjusting the distinction between the lightest and darkest tones in the image. You can choose a value in the range of -100% to +100%. The higher the positive value the lighter the light areas become and the darker the dark areas become.
- Saturation - adjusts the purity of color (the number of colors used to create a particular color). You can choose a value in the range of -100% to +100%. Positive values increase the saturation (purity); negative values decrease the saturation.

- GammaCorrect - enhances detail in the image by adjusting the middle tones without affecting the darkest and lightest areas. You can choose a gamma value in the range of 1 to 499. The larger the number, the greater the adjustment will be.
- HistoContrast - adjusts the number of pixels per gray level to create a linear relationship between gray levels. This effect can bring out the detail in dark areas of the image. You can choose a value in the range of -100% to +100%.
- Hue - adjusts the main characteristic of a particular color that distinguishes it from other colors. You can choose a value in the range of -360 to +360.
- HistoEqualize - redistributes shades of colors to adjust imbalances. It makes the darkest colors black and the lightest colors white and stretches the colors in between. It is often best to equalize a scanned image first to improve its appearance before applying other effects.
- Flip - flips the image horizontally (the image will appear upside down).
- Reverse - flips the image vertically, creating a mirror image of the original.
- Rotate - you can choose a value in the range of -360 to +360. Negative values rotate the image counterclockwise. Positive values rotate the image clockwise.
- Shear - applies the look of three-dimensionality to the image, while maintaining the original size and shape. You can choose a value in the range of -45 to +45. Negative values apply the effect to the top and left directions, positive values apply the effect to the bottom and right directions. Shear applies its effect only along the horizontal and vertical planes.
- AddNoise - creates a granular effect that adds texture to a flat or overly blended picture. You can choose a value in the range of 0 to 100.
- Average - converts each pixel in the image to the average of itself and the pixels to the right and bottom. The result is a blurring of the image. You can choose a value in the range of 1 to 100.
- Sharpen - enhances the edges and brings out detail. The higher the number, the greater the sharpening. You can choose a value in the range of -100 to +100.
- Halftone - converts the image to a black and white (1 bit/pixel) image in which different shades of gray (luminances) are represented by different patterns of back and white pixels. Denser dot patterns of white represent higher luminances (lighter areas of the image). Denser dot patterns of black dots are used represent lower luminances (dark areas of the image). Adjusting the slider adjusts the angle of the dot patterns (from 0 to 360 degrees). Simulates the image's continuous tone quality using varying hues and combinations of the process (subtractive) colors. You can choose a value in the range of -360 to +360.
- Median - reduces the amount of graininess in an image. It does so by converting each pixel in the image to the midpoint of itself and some number of pixels to the right and bottom. The result is a blurring of the image. You can choose a value in the range of 1 to 100.
- Emboss - converts the image to a raised relief style with its light source directed from the top left. The slider adjusts the depth of the embossing. You can choose a value in the range of 0 to 100.
- Grayscale - represents the image using up to 256 shades of gray.
- Invert - inverts the colors in the image as on a photographic negative.
- Mosaic - converts the image to a grid of square blocks of color. You can choose a value in the range of 1 to 100. The higher the number, the larger the blocks will be.
- Posterize - reduces the color resolution, which is the number of shades of color that can be displayed simultaneously. Gradations are removed, creating areas of solid colors or gray shades. You can choose a value in the range of 2 to 64. The lower the number, the more pronounced the effect will be.

Value type
Use the slider to adjust the value of the effect selected in the Effect Library listing window. You can also type in a numeric value. Note that some effects are not adjustable.

Add
Click this button to add the item to the Effect Profile listing window.

Click this button to remove the effect from the Effect Profile listing window

Click this button to move the effect up one position in the effect profile.

Click this button to move the effect down one position in the effect profile.

Effect Profile listing window
Lists the sequence of effects that will be performed to produce the combined effect selected in the profile list.

Profile list
Lists all currently defined effect profiles.

OK
Saves your changes and close the Image Processing window.

Cancel
Closes the Image Processing window without saving your changes.

Help
Displays online assistance for this window.

Apply
Applies the current effect profile to the original image and display the results in the Processed Image window for comparison.

Delete Profile
Removes the selected profile from the profile list

Save Profile
Saves the current profile and add it to the profile list.

Effects Gallery Sub-tab Procedures

The following procedures can be performed on this form.

Create an Effect Profile

1. Open Multimedia Capture and display an image. For more information, refer to Open Multimedia Capture on page 1343.
2. Verify the **Processing Profile** drop-down list (upper right) is empty. Otherwise, you will be modifying an existing profile instead of creating a new one.
3. On the Photo or Graphic tab, click [Process]. The Image Processing window opens.

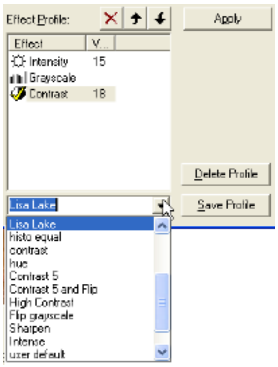
4. Select an entry in the Effect Library listing window. If the effect is adjustable, proceed to step 5. If the effect is not adjustable, proceed to step 6.

Note: The effect is adjustable if one or more fields display below the Effect Library listing window.

5. Adjust the intensity of the effect.
6. Click [Add] to add this effect to your new profile.
7. Repeat steps 4-6 for each effect you want to add to the new profile.
8. To view the result of the entire effect profile, click [Apply].
9. Enter the name of the new profile and click [Save Profile].
10. Click [OK].

Modify an Existing Effect Profile

1. Open Multimedia Capture and display an image. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo or Graphic tab, click [Process]. The Image Processing window opens.
3. Select the effect profile from the drop-down list.



4. To delete the effect, click .
5. To change the value of the effect, you must delete the effect first and then add the effect with a new value.

   For example, if you have an effect that sharpens an image by a value of 10 and you want to modify it to sharpen the image by a value of 12, you cannot simply change the value of the effect. You must first delete the sharpen effect with a value of 10 and then add the sharpen effect with the value of 12.
6. To change the order effects display, select an effect, and click the correct button.
   - Moves the entry up one position in the list.
   - Moves the entry down one position in the list.
7. Click [Save Profile].

Delete an Effect Profile

1. Open Multimedia Capture and display an image. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo or Graphic tab, click [Process]. The Image Processing window opens.
3. Select an entry from the profile list drop-down list.
4. Click [Delete Profile].

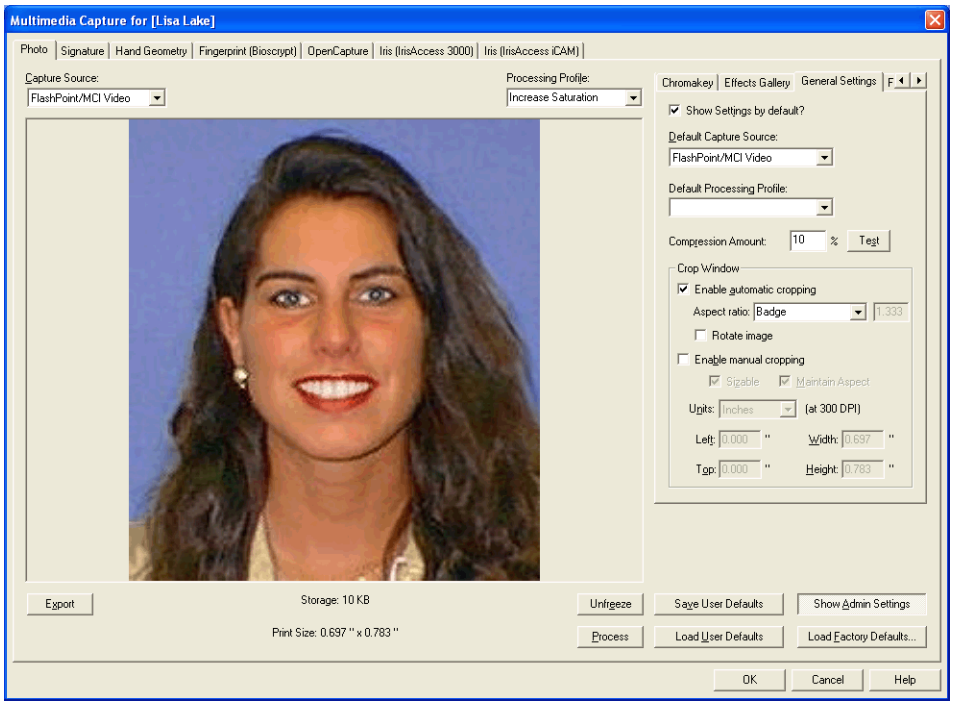
General Settings Sub-tab

The General Settings sub-tab allows you to configure:

- Which capture source (view) is automatically selected when the capture window is launched.
- Whether or not the settings will be automatically shown when the capture window is launched.
- Whether automatic cropping will be used.
- Whether manual cropping will be used.
- For automatic cropping: whether cropped images will be automatically rotated so that the eyes are level in the photograph.
- The amount of compression to be applied to bitmapped images with more than 256 colors before they are stored in the database.

Note: Image cropping only applies to bitmapped images (also known as raster images). It is NOT recommended to crop vector images.

- The size, location, and behavior of the crop window (the rectangle used for specifying which rectangular portion of the current image will be stored into the database or exported to an image file on disk).
- The units used when displaying the width and height of the portion of the image that will be stored in the database or exported to an image file on disk.
- The aspect ratio of the automatic crop window.



Show Settings by default

When this check box is selected, all settings sub-tabs applicable to the current capture source will be displayed. When this check box is not selected, only the Chromakey and Effects Gallery sub-tabs will be displayed. If you change the value of this field, you must click [Save User Defaults] button for the change to take effect.

Default Capture Source

From the drop-down list, choose which capture source you want the system to automatically default to when Multimedia Capture opens.

Default Processing Profile

From the drop-down list, choose which effect profile you want to apply to the captured image when no effect profile is chosen. Effect profiles are defined in the Image Processing window.

Compression Amount ___%

Enter the amount of compression to be applied to the captured bitmapped image (i.e. cardholder photo, bitmapped signature or layout graphic). A captured photo contains a great deal of color information so a large amount of computer disk space is required to store the photo. Compression is the process of reducing the disk space requirement.

You can choose a number between 0 and 100 to balance compression and image quality. Entering 0 (minimal compression) will yield the highest quality image with the largest disk space

requirement. Entering 100 (maximum compression) will result in the poorest quality image, but it will take up very little disk space. Refer also to the **Test** push button. The default value for this field is 10.

Compression applies only to bitmapped images with more than 256 colors. A different compression (PNG) is used for bitmapped images with 256 colors or less, which has a fixed quantity.

Test

Click this button to open the Test Compression window from where you can adjust the captured bitmapped image to achieve the best balance of image quality and disk space required. This applies only to bitmapped images with more than 25 colors.

Crop Window

The crop window displays as a rectangle superimposed over the multimedia window. It is used to select the portion of the captured image that will be saved or exported. With manual cropping, you can change the size and position of the crop window to best frame the subject. With automatic cropping, the frame is automatically sized and positioned to produce a well cropped image. However, you can override the cropped window using the manual crop sizing functions. Image cropping applies only to bitmapped images. It is not recommended for vector images.

Enable automatic cropping

When this check box is selected, the crop window is automatically displayed, cropping the captured photograph to frame the face and shoulder area of the subject. The cropped image area is pre-configured based on the default **Aspect ratio** setting.

During automatic cropping, each photograph is analyzed to ensure that it satisfies the conditions required to produce a well cropped image. For more information, refer to Image Requirements for Automatic Cropping on page 1357.

Aspect ratio

Select the aspect ratio (height-to-width) for the crop window or create a custom setting. Aspect ratios can be expressed as ratios, such as 4:3, or as numbers, such as 1.33. Available options include:

- Badge - select to use an **Aspect ratio** of 1.33 for badge images and several types of driver's licenses.
- Passport - select to use an **Aspect ratio** of 1.28 to satisfy requirements for other types of driver's licenses and numerous international passport agencies.
- Mugshot - select to use an **Aspect ratio** of 1.25.
- Custom (User defined) - When this option is selected, the field containing the value of the **Aspect ratio** is enabled allowing you to type in your desired aspect ratio (may be configured within a range of 1.25 to 1.34).

Rotate image

For automatic cropping: select to enable automatic image rotation. If needed, the captured image will be automatically rotated such that the eyes are level in the photograph.

Enable manual cropping

When this check box is selected, the crop window is displayed. Otherwise, the crop window is hidden, the whole captured image is saved or exported, and the **Sizable** and **Maintain Aspect** fields is dimmed.

Sizable

When this check box is selected, the crop window can be resized. This means that the values of the **Width** and **Height** fields can be changed. Manual crop adjustment may be used in conjunction with automatic cropping.

Maintain Aspect

When this check box is selected, the width-to-height ratio of the crop window will remain consistent (when you change the width, the height changes proportionally and vice versa). For example, if the width and height of the crop window are in the ratio of 2:3 and you enter a value of 67 for the width, the height will automatically become 100 if the **Maintain Aspect** check box is selected. This is because 67 and 100 have a 2 to 3 relationship. For more information, refer to the topic “Set Aspect Ratio Attributes” in the BadgeDesigner User Guide.

Units

Select the measurements in which the size is displayed. Choices include pixels, inches or millimeters.

Left

Sets the position of the left border of the crop window. You can also move the left border directly and this value will be automatically updated to reflect the change.

Top

Sets the position of the top border of the crop window. You can also move the top border directly and this value will be automatically updated to reflect the change.

Width

Sets the width of the crop window. You can also move the left or right border directly and this value will be automatically updated to reflect the change.

Height

Sets the height of the crop window. You can also move the top or bottom border directly and this value will be automatically updated to reflect the change.

General Settings Sub-tab Procedures

The following procedures can be performed on this form.

Enable Automatic Cropping

Automatic cropping places the crop window to automatically frame the face and shoulder region in the cardholder's photograph. Green crosshairs are displayed to mark the eye locations in the photo.

With automatic cropping, cropped image resolution is based on a selectable, pre-configured aspect ratio which provides standardized cropping across all cardholders and requires less time and effort from the badge operator.

To enable automatic cropping, select the **Enable automatic cropping** check box on the General Settings sub-tab.

Assumptions:

- Photos are captured of the cardholder's head including at least the top of the shoulders.
- The cardholder’s eyes must be visible.

- There is only one face in the image.
- The background is not too busy.
- The image is in color.

Automatic Image Rotation

If the **Rotate image** check box is selected, the captured image is automatically rotated such that the eyes are level in the photograph.

Image Requirements for Automatic Cropping

If a captured image meets the requirements for automatic cropping, the crop window is displayed. However, if the requirements for automatic cropping are not met, an error message is displayed describing the adjustments which need to be performed. Additionally, the crosshairs used to locate the eyes are red rather than green to indicate an error has occurred. For example, if the cardholder is too close to the capture device an error is generated.

- The image dimensions must not be too small.

  Minimum image resolution for automatically cropped images must be no less than 242 x 322 pixels (width x height). Typically, smaller images have been imported. In practice, a minimum image resolution of 640 x 480 is recommended.

- The image dimensions must not be too large.

  A warning is reported if the image resolution is greater than two (2) megapixels (e.g., 1600 x 1200 pixels). Large images require a considerable amount of time to process and it is recommended to decrease the image resolution. The operator is given the option to continue or to stop processing.

- The eyes of the cardholder must be located in the image.
- The cardholder's head must not be too close to the left or right edge of the photograph.
- The cardholder's head must not be too close to the top or bottom edge of the photograph.
- The cardholder must not be too far away from the capture device.

The farther the cardholder is located from the capture device, the less the distance between the eyes. There must be a minimum eye separation of 60 pixels to produce acceptable quality images.

- The cardholder must not be too close to the capture device.

  You must be able to fit the crop window within the image.

- The cardholder's head must not be tilted side-to-side more than 17º for eye location.

Correct Imperfect Eye Detection

The crosshairs displayed on the eye locations allow you to accurately correct imperfect eye detection by re-sizing the crop window. For more information, refer to Resize the Crop Window on page 1358.

IMPORTANT: Manual adjustment of the crop window may be done using the **Height** and **Width** controls but this will cause the default aspect ratio to be overridden. For more information, refer to Prevent Manual Crop Adjustment on page 1359.

Enable Manual Cropping

You can manually crop images if manual cropping is enabled and the image is bitmapped. To enable manual cropping, select the **Enable manual cropping** check box on the General Settings sub-tab. The crop window will display in the image.

If you cannot see the crop window, it may be so large that it encompasses the entire image. Simply resize the crop window.

Resize the Crop Window

To resize the crop window, the **Sizable** check box must be selected on the General Settings sub-tab.

You can resize the crop window using your mouse or, if more accuracy is required, you can enter the exact width and height of the crop window on the General Settings sub-tab.

To resize the crop window using your mouse, hover the mouse over the perimeter of the crop window. In some cases, the crop window encompasses the entire image you so may need to hover the mouse over the perimeter of the image. When the cursor changes to a double arrow, left-click on the crop window and drag it to the desired size.

Move the Crop Window

If the crop window is enabled, you can move the crop window using your mouse. Simply place the cursor inside the crop window, left-click and drag the crop window to the new location.

If more accuracy is required, you can enter the exact coordinates of the crop window on the General Settings sub-tab. Crop window coordinates are relative to the distance from the left side of the image and the distance from the top of the image. Crop window coordinates and unit of measure are entered on the General Settings sub-tab.

Adjust Image Compression

The following procedure applies only to images that are bitmapped and contain more than 256 colors.

1. Open Multimedia Capture and display an image. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo, Signature or Graphic tab, click the General Settings sub-tab.

Note: The [Show Admin Settings] button must be depressed in order to view the General Settings sub-tab.

3. If your capture source is live video, click [Freeze] because compression can be applied only to still images. Otherwise, skip to step 4.
4. On the General Settings sub-tab, click [Test]. The Test Compression window opens. The left image is uncompressed and the right image is compressed.
5. Adjust the **Compression Amount** slider to achieve the optimal balance between the amount of compression and image quality. Moving the slider to the right (higher numbers) increases the amount of compression and lowers both the image quality and the database space required. Each time you reposition the slider, click [Compress] to see the effect on the image.
6. When you find the best balance between image quality and disk space, click [OK].

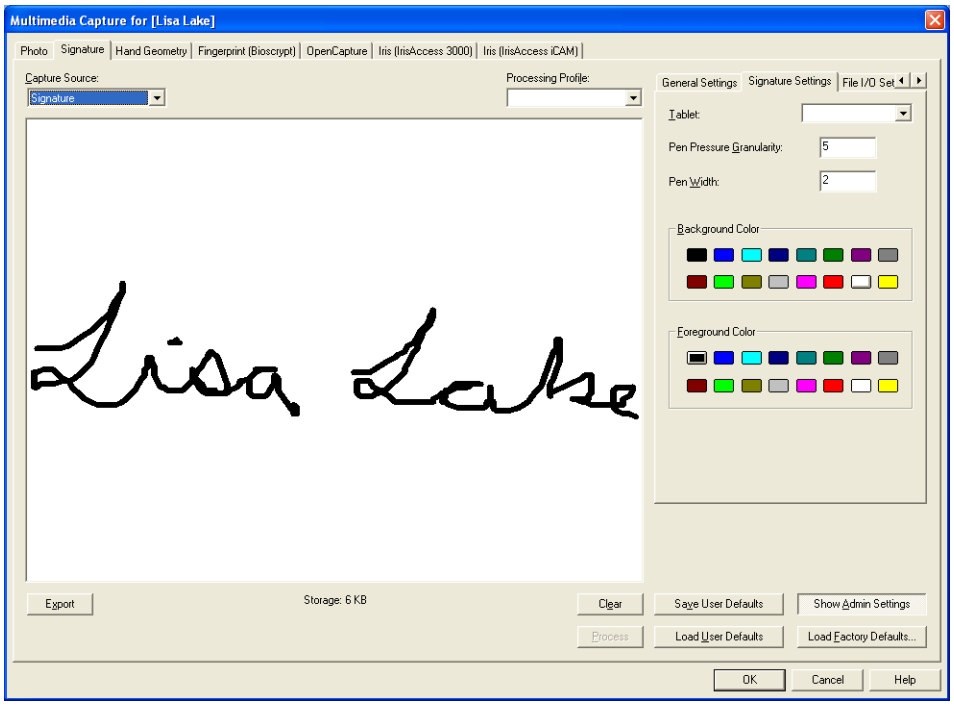
Prevent Manual Crop Adjustment

Permissions must be set to allow the badge operator to manually adjust the crop window.

To prevent operators from manually performing crop adjustment, and thereby overriding the crop window, permissions are provided to lock the usage of the **Manual crop** function. The **Advanced** option of the Capture Cardholder Permission Groups may be used to control access to all settings of the General Settings tab. The automatic cropping feature options are placed on the same tab so that enabling or disabling of automatic cropping can be controlled via permissions.

Signature Settings Sub-tab

The Signature Settings sub-tab allows you to capture cardholder's signatures. This sub-tab is displayed only when the Signature form is displayed and the "Signature" capture source is selected.



Tablet

Select the type of signature tablet you are using. Most signature tablets are of the “Wintab” type. Choices include tablet families supported by the system.

Pen Pressure Granularity

Enter the number of colors in the gradient between the darkest and the lightest colors in the signature. A granularity of 1 causes the signature to have no color variation. The maximum granularity (120) will provide the smoothest color transitions.

Pen Width

Enter the base width for either pen strokes or mouse strokes. The larger the number, the wider the line. Because this is just a base value, you can still vary the width of the stroke by varying the writing pressure. Pressing very hard causes the stroke to be a little thicker; pressing very lightly makes the stroke a little narrower.

Background Color

Select the “paper” color for signature capture. This is the color of the multimedia window in which the signature is written. The background color does not get stored with the signatures in the database; it is only used in the multimedia window.

Foreground Color

Select the “pen” color for signature capture. This is the actual pen color for the cardholder signature stored in the database. It is also the color used to print the signature in the cardholder’s screen if the badge layout is configured to use the captured color.

Signature Settings Sub-tab Procedures

The following procedures can be performed on this form.

Record a Signature

If the signature will be captured using a signature tablet and stylus, make sure that they are attached to your computer and properly configured.

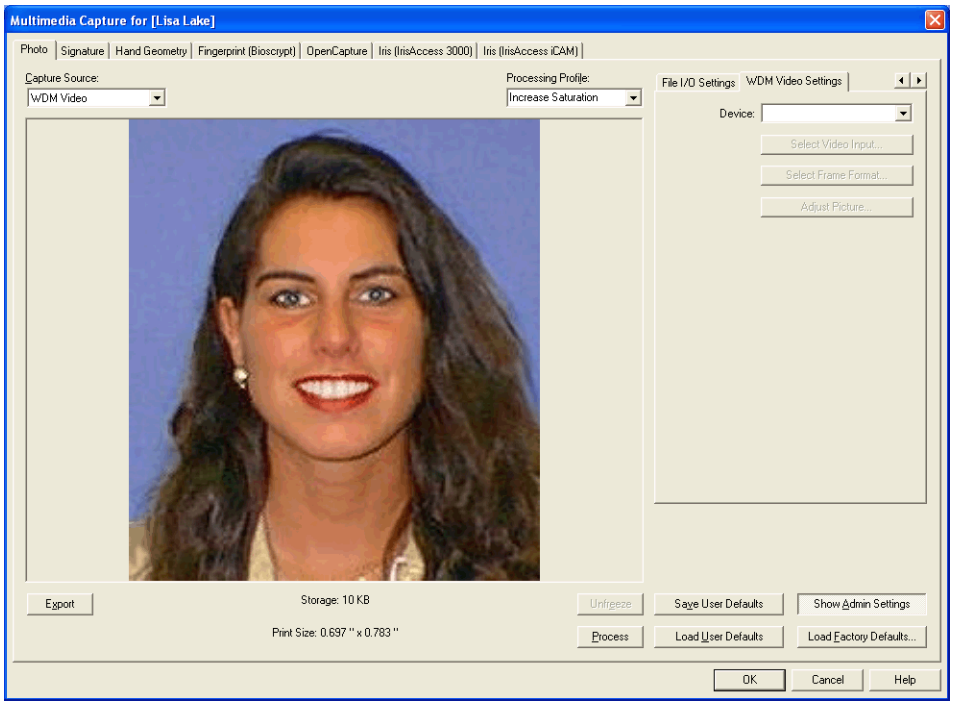
1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Signature tab.
3. Select "Signature" from the **Capture Source** drop-down list.
4. Click the General Settings sub-tab.

Note: The [Show Admin Settings] button must be depressed in order to view the General Settings sub-tab.

5. If it is not already checked, select the **Maintain Aspect** check box.
6. Click the Signature Settings sub-tab.
   a. Select the signature tablet from the **Tablet** drop-down list.
   b. Adjust the pen pressure granularity, pen width and color settings. For more information, refer to Signature Settings Sub-tab on page 1359.
7. On the Signature form, click [Sign]. If a previous signature exists you need to click [Clear] first.
8. Do one of the following:
   - If you are using a signature tablet and stylus, apply your signature to the table as you would use a pen on paper.
   - If you are using the mouse, write your signature by clicking/dragging the mouse. Just as you might lift the pen from the paper when signing your name, press and release the left mouse button as needed.
9. Click [Stop] when you finish entering your signature. The system will enlarge or reduce the signature display to fit the multimedia window while maintaining the aspect ratio.
10. Do one of the following:
    - If you are not satisfied with the results, click [Clear] and change the pen pressure granularity or pen width if necessary. Repeat steps 7-9 to capture the signature again.
    - If you are satisfied with the results, click [OK] to save the signature.

WDM Video Settings Sub-tab

The WDM Video Settings sub-tab allows you to configure the main set of options for the "WDM Video" capture source. When the "WDM Video" capture source is selected, live video from the currently selected video input of the currently selected WDM video capture device will be displayed in the multimedia window. This sub-tab is displayed only when the "WDM Video" capture source is selected.



Device

Choose a specific WDM video capture device. Choices include all WDM video capture devices that are currently installed on this workstation. Live video from the currently selected video input will then be displayed in the multimedia window.

Select Video Input

Click this button to open the Select Video Input window from where you can select which video input to use.

Select Frame Format

Click this button to select a frame format. For some WDM devices, a window will open from where you can select the spatial resolution (number of pixels across and down) and the pixel format of captured video frames. For devices that do not allow you to adjust the frame format, the system automatically selects the frame format that has the largest spatial resolution and a pixel format with the most color information.

Adjust Picture

Click this button to adjust picture quality attributes such as hue, brightness and contrast. Depending on which WDM device you are configuring, a properties window will be displayed from where you can adjust these settings.

WDM Video Settings Sub-tab Procedures

The following procedures can be performed on this form.

Configure WDM Video Settings

You should first complete this procedure using a test subject (person). Once you have optimized the settings for your physical environment, you shouldn't need to modify them unless you change the surroundings. Adjustments for an individual's skin tone, hair color or clothing color can be made using the Image Processing window after the image has been captured.

Before you begin, make sure that your camera and flash unit are powered on and properly configured for use.

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo, Signature or Graphic tab, select "WDM Video" from the **Capture Source** drop-down list.
3. Click the WDM Video Settings sub-tab. (The [Show Admin Settings] button must be depressed in order to view the WDM Video Settings sub-tab.)
4. From the **Device** drop-down list, select the WDM video capture device that you want to configure settings for.
5. Click [Select Video Input]. The Select Video Input window opens.
6. In the Select Video Input window, choose which video input you want to use.
7. Click [Select Frame Format]. For some WDM devices, a window will open from where you can select the spatial resolution (number of pixels across and down) and the pixel format of captured video frames. For devices that do not allow you to adjust the frame format, the system automatically selects the frame format that has the largest spatial resolution and a pixel format with the most color information.
8. Click [Adjust Picture]. Depending on which WDM device you are configuring, a properties window opens, from where you can adjust these settings. From this window, adjust picture quality attributes such as hue, brightness and contrast.
9. If you want to save your settings so that they will be automatically displayed each time you select the WDM Settings sub-tab, click [Save User Defaults].

Note: If you want to use the factory-set values for these fields, click [Load Hardware Defaults] button. The sliders will be repositioned accordingly.

Capture an Image Using Live Video

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo or Graphic tab, select either "FlashPoint/MCI Video" or "WDM Video" from the **Capture Source** drop-down list.

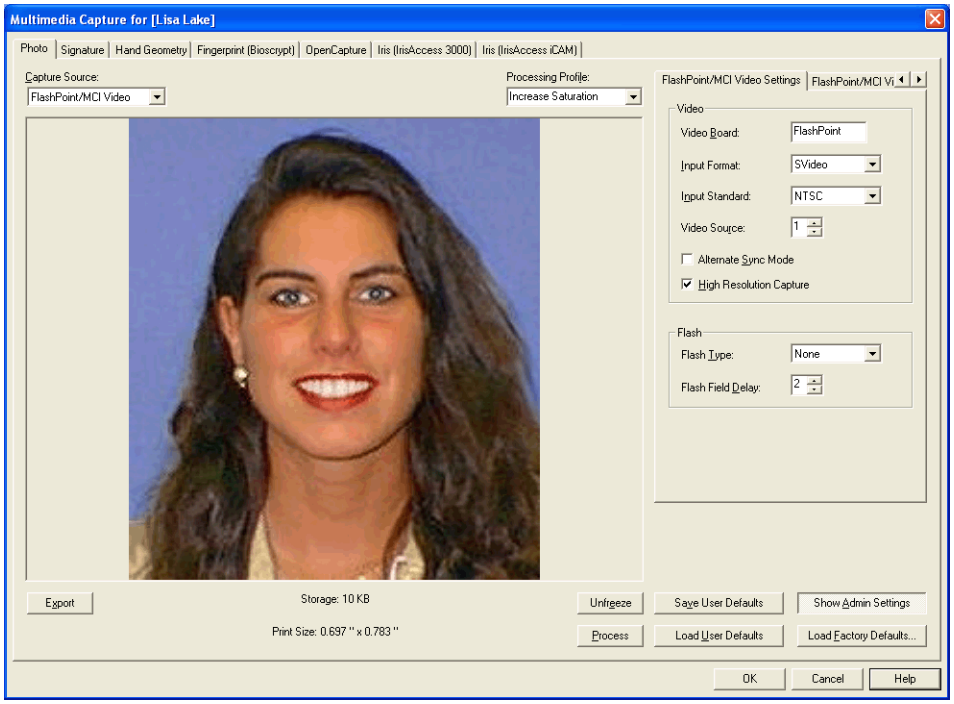
Note: The [Show Admin Settings] button must be depressed in order to view the sub-tab.

3. Click the General Settings sub-tab.
4. If an image displays, click [Clear].
5. Physically position the test subject so their head and shoulders appear in the Multimedia Capture window. Click [Freeze].
6. Using your mouse, adjust the crop window to frame the subject. If the crop window is enabled, it displays as a rectangle over the image. For more information, refer to Enable Manual Cropping on page 1358 and Resize the Crop Window on page 1358.
7. If you want to retake the photo, click [Unfreeze] and repeat steps 4-5.

8. When you are satisfied with the image, click [OK].
9. If you want to adjust the photo quality, click [Process].

FlashPoint/MCI Video Settings Sub-tab

The FlashPoint/MCI Video Settings sub-tab allows you to configure the main set of options for the "FlashPoint/MCI Video" capture source. When the "FlashPoint/MCI Video" capture source is selected, live video from the FlashPoint/MCI video device will be displayed in the multimedia window. This sub-tab is displayed only when the "FlashPoint/MCI Video" capture source is selected.



Video Board

Enter the name of the driver for your video capture board. The default is "FlashPoint." Contact your Lenel representative for assistance if you have a video board that is not an Integral Technologies FlashPoint board.

Input Format

Select the format of the incoming video signal. Choices include:

- RGB - accepts separate inputs for the red, green and blue components.
- Composite - mixes the red, green and blue signals to produce a color image.
- SVideo - an analog video interface standard that separates the signal into two components, brightness and color.

Input Standard

Select the incoming video signal standard. Choices include:

- NTSC - the U.S. standard
- PAL - the European standard

Video Source

Select which video connector the incoming video signal is to be captured from. (Video connectors are numbered starting with zero.)

Alternate Sync Mode

When this check box is selected, incoming video is routed through special video stabilizer circuitry in the FlashPoint video capture board. This allows you to capture video from video sources emitting “messy” video signals.

For example, video that comes from a VCR may constantly jump around on the screen if the VCR has a dirty play head, poor tracking or a worn-out tape in it. If the **Alternate Sync Mode** check box is selected, the video will stop jumping around and settle down to a stable picture, although there is usually a band of static (snow) at the bottom because some rows of the incoming video frames are lost during the stabilization process.

High Resolution Capture

When this check box is selected, you can capture photos at the maximum resolution of 640 by 480 pixels instead of 320 by 240 pixels. (The high resolution photos will print on the cards at sizes larger than 0.6” by 0.8” with better quality, but at the price of a 300 to 400% increase in disk storage requirements.) To use high resolution capture you must:

- Use a Flashpoint board. Users with FlashPoint boards can now capture photos at a maximum resolution of 640 by 480 pixels instead of 320 by 240 pixels.
- Have a Desktop area that is at least 1024 by 768 pixels. Users who want to use high resolution capture must have a Windows desktop area that is at least 1024 by 768 pixels because a 640 by 480 pixel capture window and capture window user interface will not fit onto a 800 by 600 pixel desktop at the same time.
- Use a flash type other than “Universal.” To capture in high resolution, a flash type other than “Universal” must be used because Universal flash is capable of illuminating only one video field, i.e. every other row of pixels or 240 lines, within a high resolution video frame.

Flash Type

Select the type of flash unit connected. Your selection must match the jumper settings on the FlashPoint video capture board. For more information, refer to the your FlashPoint user guide for jumper information. Choices include:

- None - no flash unit connected. If you do not have a flash unit, you must make sure that the video capture environment contains sufficient light for the process. The maximum height is 480 when the capture is made in high resolution mode.
- Universal - triggers any standard photographic flash unit. The video capture board triggers the flash unit directly.
- CCD - flash trigger specifically for the Kodak CCD4000 camera. Instead of the flash being fired directly, the system triggers flash through the camera, a process called frame integrated flash. The maximum height is 480 when the capture is made in high resolution mode. If you choose this option, you must first configure your hardware for this capability.

When capturing with a universal flash or in low resolution capture mode, the maximum unscaled video frame height for the FlashPoint board is 240 lines of pixels.

Flash Field Delay

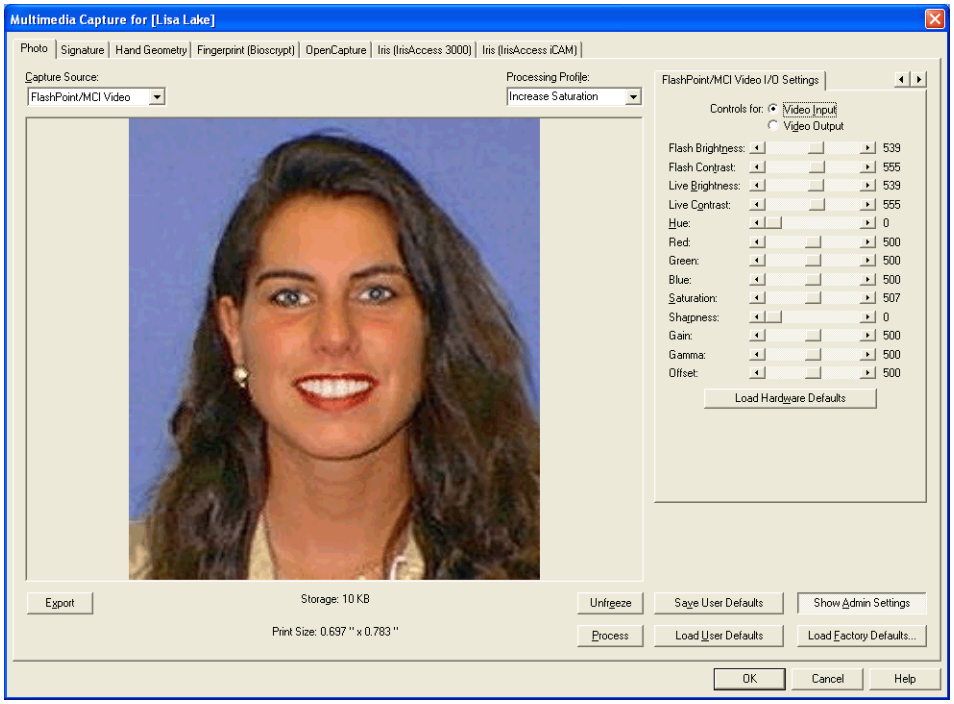
Enter the number of video fields you want the system to wait after it has fired the flash before it freezes (captures) video. This is used to synchronize a flash with the freeze-frame process so that frames will be captured while the light emitted from the flash is at its brightest.

Live video consists of pixels arranged in lines called fields. Each frame of video contains one even field and one odd field. The even field is composed of every odd numbered line of pixels,

beginning with the first (top) line. The other lines in the frame constitute the odd field. Therefore, the incoming video signal alternates between the even and the odd fields at twice the video frame rate (60 fields per second for the NTSC video standard, 50 fields per second for the PAL video standard).

FlashPoint/MCI Video I/O Settings Sub-tab

The FlashPoint/MCI Video I/O Settings sub-tab allows you to adjust the color, intensity and contrast of video captured with the “FlashPoint/MCIVideo” capture source. This sub-tab is displayed only when the “FlashPoint/MCI Video” capture source is selected.



Controls for Video Input

When this radio button is selected, the slider field settings adjust characteristics of the incoming video signal. These settings affect how the video is captured. The fields are board-dependent. A dimmed field means that your video capture board does not support the corresponding characteristic. Possible values for all slider fields are in the range of 0 through 1000.

Controls for Video Output

When this radio button is selected, the slider field settings adjust the output video display. These settings will affect only how the video is displayed. The fields are board-dependent. A dimmed field means that your video capture board does not support the corresponding characteristic. Possible values for all slider fields are in the range of 0 through 1000.

Flash Brightness

Increases or decrease the value of all color components for the flash.

Flash Contrast

Increases or decreases the differences in brightness between the image's brightest and darkest elements for the flash.

Live Brightness

Controls the brightness for live video. Live video is darker with flash due to the reduced iris setting needed to prevent the flash from overpowering the camera. When the image is captured (by clicking the [Freeze] button), the controls switch over to the **Flash Brightness** setting.

Live Contrast

Controls the contrast for live video. When the image is captured (by clicking the [Freeze] button), the controls switch over to the **Flash Contrast** setting.

Hue

Adjusts the aspect of a color that distinguishes it from other colors. This field is useful to achieve accurate skin tones in the image.

Red

Increases or decreases the global value of the image's red component

Green

Increases or decreases the global value of the image's green component

Blue

Increases or decreases the global value of the image's blue component.

Saturation

Adjusts the amount of color (intensity) to accommodate stronger and weaker input color signals.

Sharpness

Adjusts the image to be either more focused or more blurry.

Gain

Boosts the weak input signal or decreases noise coming from a strong but noisy source, helping to enhance details.

Gamma

Provides a nonlinear contrast adjustment. A higher gamma value produces a brighter image that has less contrast. A lower gamma value produces a darker image that has more contrast.

Offset

Moves the input signal level up or down without changing the signal size, helping to enhance details. This field is useful if your camera has a nonstandard output or has a direct current offset.

Load Hardware Defaults

Click this button to change the values of all slider fields to the factory defaults set by the video board manufacturer. (If you are using a FlashPoint board, this button loads the settings last saved with the FPG application that Integral ships with their boards.)

FlashPoint/MCI Video Settings Procedures

The following procedures can be used on this form.

Configure FlashPoint/MCI Video Capture Settings

Notes: You should first complete this procedure using a test subject (person). Once you have optimized the settings for your physical environment, you shouldn't need to modify them unless you change the surroundings. Adjustments for an individual's skin tone, hair color or clothing color can be made using the Image Processing window after the image has been captured.

Before you begin, make sure that your camera and flash unit are powered on and properly configured for use.

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo, Signature or Graphic tab, select “FlashPoint/MCI Video” from the **Capture Source** drop-down list.
3. Click the FlashPoint/MCI Video Settings sub-tab.

Note: The [Show Admin Settings] button must be depressed in order to view the FlashPoint/MCI Video Settings sub-tab.

4. In the Video section, choose the settings for your video source. For more information, refer to FlashPoint/MCI Video Settings Sub-tab on page 1364.
5. In the Flash section, choose flash settings. For more information, refer to FlashPoint/MCI Video Settings Sub-tab on page 1364.
6. If you want to save your settings so that they will be automatically displayed each time you select the FlashPoint/MCI Video Settings sub-tab, click [Save User Defaults].
7. Click the FlashPoint/MCI Video I/O Settings tab to display the FlashPoint/MCI Video I/O Settings sub-tab. (The [Show Admin Settings] button must be depressed in order to view the FlashPoint/MCI Video I/O Settings sub-tab.)
8. Select the **Video Input** radio button, then adjust the slider controls to optimize the incoming video signal. You can also do the same for video output (by selecting the **Video Output** radio button and adjusting the slider controls) to optimize the video display, although these settings are typically not adjusted.

Note: If you want to use the factory-set values for these fields, click [Load Hardware Defaults] button. The sliders will be repositioned accordingly.

9. If you want to save your settings so that they will be automatically displayed each time you select the FlashPoint/MCI Video I/O Settings sub-tab, click [Save User Defaults].

Use High Resolution Analog Video Capture

To capture analog video in high resolution, you must:

- Use a Flashpoint board. Users with FlashPoint boards can capture photos at a maximum resolution of 640 by 480 pixels instead of 320 by 240 pixels. (The high resolution photos will print on the cards at sizes larger than 0.6” by 0.8” with better quality, but at the price of a 300 to 400% increase in disk storage requirements.)
- Have a Desktop area that is at least 1024 by 768 pixels. Users who want to use high resolution capture must have a Windows desktop area that is at least 1024 by 768 pixels because a 640 by 480 pixel capture window and capture window user interface won’t fit onto a 800 by 600 pixel desktop at the same time.

- Use a flash type other than “Universal”. To capture in high resolution, a flash type other than “Universal” must be used because Universal flash is capable of illuminating only one video field (every other row of pixels or 240 lines) within a high resolution video frame.

The size of the image/video display in the multimedia window varies depending on the Windows desktop area. The following applies:

- Windows desktop areas smaller than 800 by 600 pixels are no longer supported by the capture window.
- When the Windows desktop area between 800 by 600 pixels and 1024 by 768 pixels (as with the case with many laptops running mobile badging) the multimedia window is at a smaller size so everything will fit onto the screen. In this situation the image display area is 320 by 240 pixels and thus the user is unable to set analog video capture to high resolution mode.

Note: Although high resolution analog video capture is not available when the desktop area is less than 1024 by 768 pixels, the **High Resolution Capture** check box remains visible. If an attempt to select high resolution capture is made, a message will be displayed that explains why it is not available.

- When the Windows desktop area is 1024 by 768 pixels or larger the capture window is now bigger so that the image display area (the area on the left hand side) and hence the multimedia window, can be 640 by 480 pixels, allowing for high resolution analog video capture. It will be 320 by 240 pixels if the **Flash Type** is “Universal.”

Windows desktop area (pixels)	Image display description	High resolution analog video capture supported
Smaller than 800 by 600	No longer supported	No
Between 800 by 600 and 1024 by 768	320 by 240 image display (smaller)	No
1024 by 768 and larger	640 by 480 image/video display (larger)	Yes, if **Flash Type** is not “Universal”

To capture high resolution analog video:

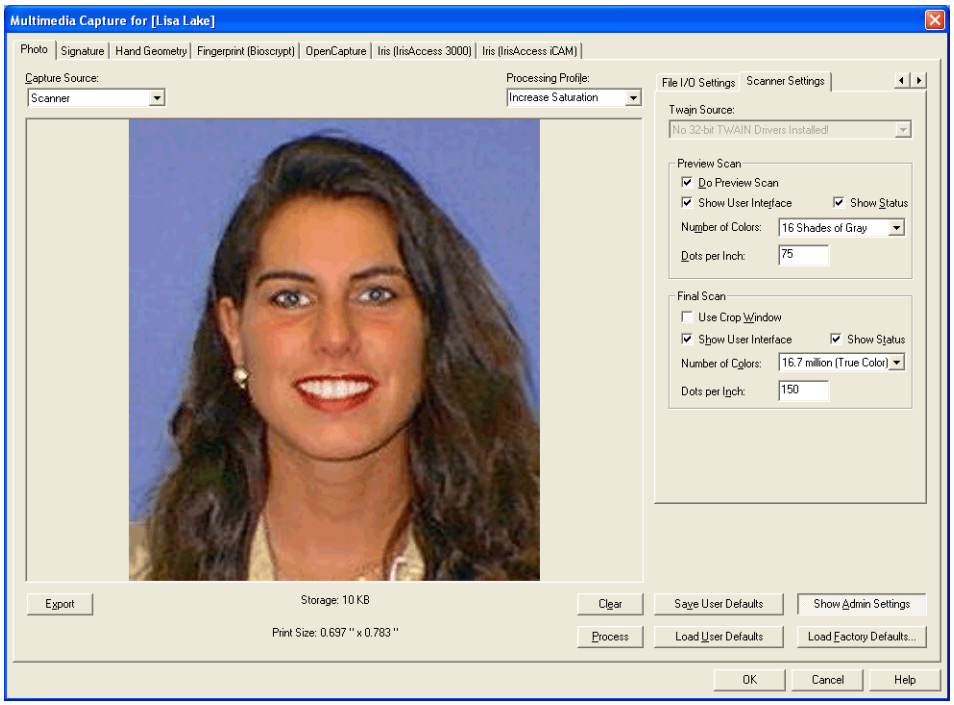
1. Make sure that the desktop area is at least 1024 pixels by 768 pixels.
2. Open Multimedia Capture.For more information, refer to Open Multimedia Capture on page 1343.
3. On the Photo, Signature or Graphic tab, select “FlashPoint/MCI Video” from the **Capture Source** drop-down list.
4. Click the FlashPoint/MCI Video Settings sub-tab.

Note: The [Show Admin Settings] button must be depressed in order to view the FlashPoint/MCI Video Settings sub-tab.

5. Select the **High Resolution Capture** check box.
6. Make sure that “Universal” is not selected in the **Flash Type** field.

Scanner Settings Sub-tab

The Scanner Settings sub-tab allows you to configure how images are scanned. This sub-tab is displayed only when the “Scanner” capture source is selected.



Twain Source

Select the name of your scanner. In order for your scanner to be listed, you must have first attached the scanner to your computer, installed the device’s Twain driver software and configured it for use. For more information, refer to your scanner’s user guide. The **Twain Source** drop-down list will list the names of both scanners and digital cameras that are configured on your system.

Preview Scan

Includes the **Do Preview Scan** check box and the upper **Show User Interface**, **Show Status**, **Number of Colors** and **Dots per Inch** fields.

Do Preview Scan

When this check box is selected, you can scan the entire original page, then position the crop window and perform a final scan on only the area enclosed by the crop window. When this check box is not selected, you can bypass the preview scan and perform only a final scan. If you deselect this check box, you can ignore the other settings in the Preview Scan section.

Show User Interface

Select this check box to be allowed to utilize the Twain driver's default user interface instead of bypassing it.

Show Status

When this check box is selected and the Twain driver supports this option, a status bar is displayed showing the status of the scan. This does not apply if you are using your Twain driver's default user interface.

Dots per Inch
Specify the final scanning resolution, expressed in dots per inch.

Number of Colors
Specify the final pixel type of the image to be scanned.

Dots per Inch
Specify the resolution for preview scanning, expressed in dots per inch.

Final Scan
Includes the **Use Crop Window** check box and the lower **Show User Interface**, **Show Status**, **Number of Colors** and **Dots per Inch** fields.

Use Crop Window
When this check box is selected, you can perform a full (final) scan of the area enclosed by the specified crop window. When this check box is not selected, you can perform a scan using the default size set by the Twain driver. If the **Do Preview Scan** check box is selected, the crop window set there is used and this option has no effect.

Show User Interface
When this check box is selected, you can utilize your Twain driver's default user interface. When this check box is not selected, your Twain driver's default user interface is bypassed.

Show Status
When this check box is selected and your Twain driver supports this option, a status bar is displayed showing the status of the scan. This does not apply if you are using your Twain driver's default user interface.

Number of Colors
Specify the final pixel type of the image to be scanned.

Scanner Settings Sub-tab Procedures

The following procedures can be performed on this form.

Preview and Scan an Image

In most situations, this is the basic process for scanning an image. Before you proceed, make sure that your scanner hardware is attached to your computer and the scanner software is installed and configured for use.

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Photo, Signature or Graphic tab.
3. Select "Scanner" from the **Capture Source** drop-down list.
4. Click the Scanner Settings sub-tab. (The [Show Admin Settings] button must be depressed in order to view the Scanner Settings sub-tab.)
5. Select the name of your scanner's drive from the **Twain Source** drop-down list.
6. In the Preview Scan section:
    a. Select the **Do Preview Scan** check box.

b. Enter values in the **Number of Colors** and **Dots per Inch** fields. It is recommended that you choose low values such as “16 Shades of Gray” and “75” dots per inch because the preview scan records the entire flatbed surface, performing a preview scan at a high resolution. A large amount of color information would require a huge amount of memory and hard disk space.

7. Position the photograph on the scanner by placing the photo flush with the corner of the scanning surface. It the photograph is oriented incorrectly, the scanned image will appear crooked in the multimedia window. If this happens, to correct the problem, you’ll need to either rescan the original image or manipulate the image using the Image Processing window.
8. Click [Preview]. The entire contents of the scanning surface will be scanned and displayed in the multimedia window (the image in the window will look mostly blank except for a small photo).
9. In the Final Scan section:
   a. Click the **Use Crop Window** check box.
   b. Enter values in the **Number of Colors** and **Dots per Inch** fields. It is recommended that you choose high values such as “16.7 million (True Color)” and “300” dots per inch, ensuring that the final captured image is of the highest possible quality.
10. Move and resize the crop window to frame the image. If the crop window is enabled, it displays as a rectangle on the image. For more information, refer to Enable Manual Cropping on page 1358 and Resize the Crop Window on page 1358.
11. Click [Scan]. The system scans the contents of the crop window.
12. To adjust the photo quality, click [Process]. For more information, refer to Image Processing Window on page 1349.

Bypass the Preview Scan Step

The following procedure is useful if you have multiple hard copies that are the same size and you want to skip multiple preview scan steps. With this procedure, you preview the first hardcopy only.

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Photo, Signature or Graphic tab.
3. Select “Scanner” from the **Capture Source** drop-down list.
4. Click the Scanner Settings sub-tab. (The [Show Admin Settings] button must be depressed in order to view the Scanner Settings sub-tab.)
5. Select the **Use Crop Window** check box.
6. Position a photograph on the scanner and click [Preview].
7. Move and resize the crop window to frame the photograph. If the crop window is enabled, it displays as a rectangle on the image. For more information, refer to Enable Manual Cropping on page 1358 and Resize the Crop Window on page 1358.
8. Deselect the **Do Preview Scan** check box.
9. Click [Save User Defaults].
10. Click [Scan]. The system scans the contents of the crop window.
11. To scan another hardcopy, place it on the scanner in the same position as the first hardcopy and click [Scan]. All subsequent scans use the crop window position you specified in step 7.

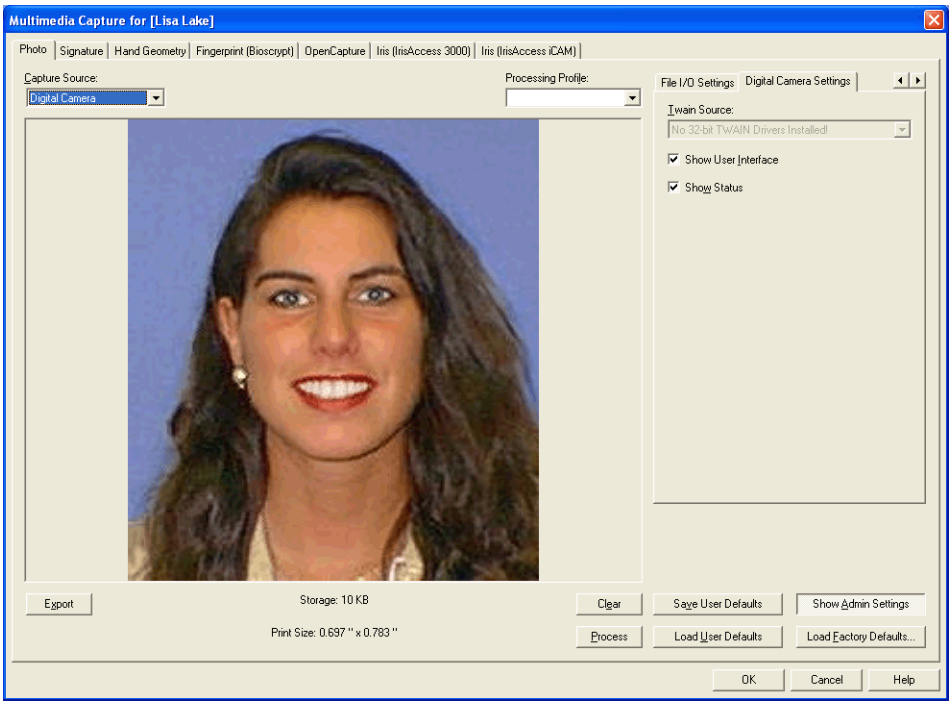
Notes: If you have a batch of photos to scan and all but a few of them are the same size, you can deselect the **Use Crop Window** check box just prior to scanning an odd-sized photo. Then move and resize the crop window and do the scan. After scanning the odd-

sized photo, reselect the **Use Crop Window** check box to return to using the crop window settings you saved as the default.

Many Twain drivers for scanners ignore dots per inch and number of color settings. For this reason, it is highly recommended that you select the **Show User Interface** check box.

Digital Camera Settings Sub-tab

The Digital Camera Settings sub-tab allows you to configure how images are downloaded from digital cameras with the “Digital Camera” capture source. This sub-tab is displayed only when the “Digital Camera” capture source is selected.



Twain Source

Select the name of your digital camera. In order for your digital camera to be listed, you must have first attached the camera to your computer, installed the device’s Twain driver software and configured it for use. For more information, refer to your digital camera’s user guide. The **Twain Source** drop-down list will list the names of both scanners and digital cameras that are configured on your system.

Show User Interface

When this check box is selected, you can utilize your Twain driver’s default user interface instead of bypassing it. It is highly recommended that you select this option.

Show Status

When you select this check box and the Twain driver supports this option, a status bar is displayed showing the status of the scan. This does not apply if you are using your Twain driver's default user interface.

Digital Camera Settings Sub-tab Procedures

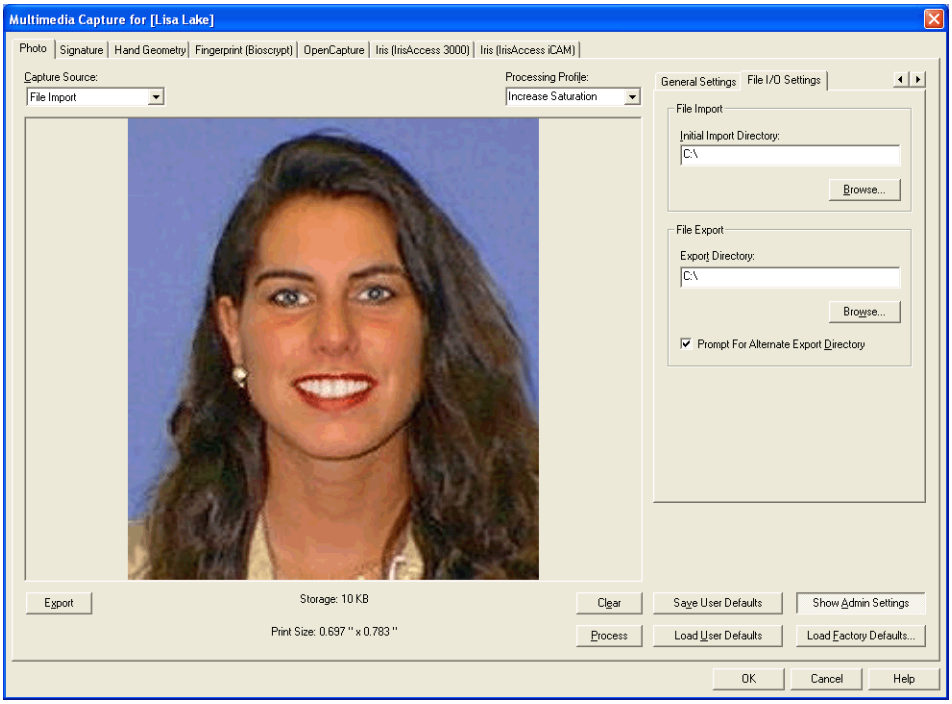
The following procedures can be performed on this form.

Capture Digital Images

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Photo tab or Graphic tab.
3. Select “Digital Camera” from the **Capture Source** drop-down list.
4. Click the Digital Camera Settings sub-tab. (The [Show Admin Settings] button must be depressed in order to view the Digital Camera Settings sub-tab.)
5. On the Digital Camera Settings sub-tab:
   a. Select the name of your digital camera from the **Twain Source** drop-down list.
   b. It is recommended that you select the **Show User Interface** check box. Otherwise, you will just download the first photo that is in the camera.
6. Click [Get Photo]. If an image displays, you need to click [Clear] first.
7. If the user interface for the digital camera software opens, adjust any settings. Otherwise, continue with the next step.
8. Take a picture of the cardholder/visitor. The image displays in Multimedia Capture.
9. Move and resize the crop window to frame the image. If the crop window is enabled, it displays as a rectangle on the image. For more information, refer to Enable Manual Cropping on page 1358 and Resize the Crop Window on page 1358.
10. To adjust the image quality, click [Process].

File I/O Settings Sub-tab

The File I/O Settings sub-tab allows you to configure the default file import directory for the “File Import” capture source and the default file export directory for all of the capture sources.



Initial Import Directory

Enter the first place (drive and directory) in which to look when importing an image file into the database.

Browse

Opens the Browse for Folder window from where you can select an initial import directory.

Export Directory

Enter the drive and directory into which image and signature files are saved when you click [Export].

Browse

Opens the Browse for Folder window from where you can select an export directory.

Prompt for Alternate Export Directory

When this check box is selected, you will be prompted with the standard File Save window when you click [Export]. The window is initialized to point to the file export directory. When this check box is not selected, the image is exported without the user being prompted for the export filename and path unless the file already exists.

File I/O Settings Sub-tab Procedures

The following procedures can be performed on this form.

Configure Multimedia Capture for File Import

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.

2. On the Photo, Signature or Graphic tab, select “File Import” from the **Capture Source** drop-down list.
3. Click the File I/O Settings sub-tab.

Note: The [Show Admin Settings] button must be depressed in order to view the File I/O Settings sub-tab.

4. Complete the File Import section.
5. If you want to save your settings so that they will be automatically display, click [Save User Defaults].

Import a Supported Image File

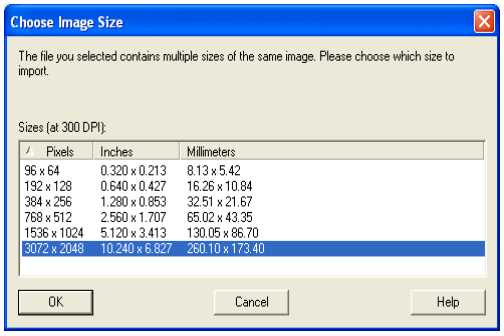
1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. On the Photo, Signature or Graphic tab, select “File Import” from the **Capture Source** drop-down list.
3. Click the File I/O Settings sub-tab.

Note: The [Show Admin Settings] button must be depressed in order to view the File I/O Settings sub-tab.

4. If an image or signature displays in the multimedia window, click [Clear]. Click [Open].
5. Select the file you want to import and click [Open]. The image displays in Multimedia Capture.
6. If the image is bitmapped and the crop window is enabled, adjust the crop window to frame the portion of the image that you want to save. To adjust the crop window, refer to Resize the Crop Window on page 1358.
7. Click [OK] twice.

Import a Multi-Resolution Image File

If the image file you are importing is a multi-resolution image the following dialog box will appear. Here you can choose what resolution you would like the image to be imported as.



Import a Non-Supported Image File

A large number of image file formats are supported. However, you may encounter a format that you wish to import that is not supported. Contact your Lenel representative for assistance if you would like support for a non-supported image file format to be added. This procedure details how to import an image that is in a file format that is not supported. For more information, refer to Supported Image Formats on page 1377.

1. Save a temporary copy of the image in a supported format. Do this using a third party graphics editor/conversion application, preferably the one used to create the image.
   It is strongly suggested that you create the temporary file in a format that preserves original image quality. Here are a few guidelines to accomplish this:
   - If the image is non-photographic and doesn't look jagged when scaled larger (i.e., not a bitmap):
     - Use EMF if you can otherwise, use WMF or DXF.
     - Images created with CAD programs (like floor plans for buildings) and drawn images (like company logos) fall into this category.
   - If the image is photographic or is known to have more than 256 colors:
     - Use 16.7 million color BMP (i.e., 24-bits/pixel or true color BMP)
     - Use JPEG with a minimal amount compression if you have low disk space.
     - Scanned images and images captured from a video camera or digital camera fall into this category.
   - Otherwise, use 16 color or 256 color BMP (i.e., 4 or 8 bits/pixel BMP).
     - The number of BMP colors should be greater than or equal to the number of colors used in the image.
     - Hand-drawn bitmapped images and photographic GIF images fall into this category.
2. Import the temporary file. For more information, refer to Import a Supported Image File on page 1376.
3. Delete the temporary file.

Supported Image Formats

The following table lists the image formats that you can import. If the file format you are working with is not identified by bits per pixel, refer to the Bits Per Pixel and Number of Colors Information on page 1379 to determine color information.

Supported Image Formats

Format name	Common file extension(s)	Sub-formats supported (compression type/bits per pixel)
Adobe Photoshop	PSD	None/1, 8, 24
Auto CAD	DXF	
CALS Raster	CAL	CCITT Group 4/1
Delrina WinFax Group 3	FAX	CCITT Group 3/1
Delrina WinFax Group 4	FAX	CCITT Group 4/1
Encapsulated PostScript	EPS	• PostScript Raster images/1,8 • Embedded TIFF images/(See TIFF format) Raster image information only, vector image information is ignored
FAX Group 3	FAX	• 1-Dimensional Group 3 without header (raw)/1 • 2-Dimensional Group 3 without header (raw)/1

Supported Image Formats (Continued)

Format name	Common file extension(s)	Sub-formats supported (compression type/bits per pixel)
FAX Group 4	FAX	CCITT Group 4 without header (raw)/1
GEM Image	IMG	NONE/1
IOCA or IBM Image Object Content Architecture	ICA	• MO:DCA wrapper with embedded CCITT Group 3/1 • MO:DCA wrapper with embedded CCITT Group 4/1 • No MO:DCA wrapper/1
JFIF or JPEG File Interchange Format	JPG/JIF	• Progressive JPEG/8 (YUV 4:0:0 grayscale), 24 (YUV 4:4:4, 4:2:2, 4:1:1 color) • Non-progressive JPEG/8 (YUV 4:0:0 grayscale), 24 (YUV 4:4:4, 4:2:2, 4:1:1 color)
JPEG Tagged Interchange Format	JTIF	Non-progressive JPEG/8 (YUV 4:0:0 grayscale), 24 (YUV 4:4:4, 4:2:2, 4:1:1 color)
Kodak FlashPix	FPX	• NONE/8, 24 • JPEG
Kodak Photo CD	PCD	NONE/8, 24
LEAD CMP	CMP	• Progressive CMP/1,8,24 • Non-progressive CMP/1,8,24
Macintosh Pict Format	PCT	NONE/1, 4, 8, 24
MacPaint	MAC	NONE/1
Microsoft Paint	MSP	NONE/1
OS/2 Bitmap	BMP	1.x and 2.x formats/1, 4, 8, 24
Portable Network Graphics	PNG	PNG/1, 4, 8, 16, 24, 32
SUN Raster Format	RAS	NONE/1, 4, 8, 24, 32
TIFF or Tagged Interchange File Format/Multipage TIFF	TIF/MPT	• Uncompressed/1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32 • RLE/1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32 • CCITT/1 • 1-dimensional CCITT Group 3/1 • CCITT Group 4/1 • JTIF (Non-progressive JPEG)/8 (YUV 4:0:0 grayscale), 24 (YUV 4:4:4, 4:2:2 or 4:1:1 color)
Truevision TARGA	TGA	• Uncompressed/8, 16, 24, 32 • RLE/8, 16, 24, 32
Windows Bitmap	BMP/DIB	• Uncompressed/1, 4, 8, 16, 24, 32 • RLE/1, 4, 8

Supported Image Formats (Continued)

Format name	Common file extension(s)	Sub-formats supported (compression type/bits per pixel)
Windows Enhanced Metafile	EMF	• Uncompressed/1, 4, 8, 16, 24, 32 • RLE/1, 4, 8
Windows Metafile	WMF	• Uncompressed/1, 4, 8, 16, 24, 32 • RLE/1, 4, 8
WordPerfect Format	WPG	RLE/1, 4, 8 (Raster image information only, vector image information is ignored)
Zsoft PCX / Multipage PCX	PCX/DCX	RLE/1, 4, 8, 24

Bits Per Pixel and Number of Colors Information

Bits per pixel	Number of colors	Description
1	2	Monochrome
2	4	CGA
3	8	
4	16	EGA/VGA
5	32	
6	64	
7	128	
8	256	256 color VGA/256 gray levels
16	65,536	High Color
24	16,777,216	True Color
32	16,777,216	True Color with 8 bits of alpha information. The alpha information is ignored.

Notes About Specific Image Formats

- EPS & WPG Image Formats

  OnGuard provides partial support for the EPS (Encapsulated PostScript) and WPG (WordPerfect Format) formats. While EPS and WPG files can contain raster (bitmap) and vector (text, line, and shape drawing commands) information, OnGuard applications can only read raster information.

  If you want to import EPS or WPG files that contain vector information you should convert the files to EMF (Windows Enhanced Metafile) or WMF (Windows Metafile) format and import those files instead.
- EMF, WMF, & DXF Image Formats

EMF and WMF files contain raster (bitmaps) and/or vector (text, line, and shape drawing commands) data. DXF files contain vector data only.

OnGuard supports EMF, WMF, and DXF file import. This means that:

- Badge layout graphics, cardholder photos, and cardholder signatures can be imported as WMF, EMF, and DXF files.
- Vector images can be imported and remain vector images instead of being converted to bitmaps. However, the signature settings, image processing, chromakey, and the crop window are disabled when a vector image is imported.

- GIF & LZW Image Formats (Not Supported)

  As the result of Unisys licensing the LZW compression technology, GIF (Graphics Interchange Format), and LZW compressed TIFF formats are not supported.

Hand Geometry Form

The access control hand readers supported by OnGuard include the HandKey II, HandKey (ID3D), and HandKey-CM readers.

Hand Geometry License and Permissions

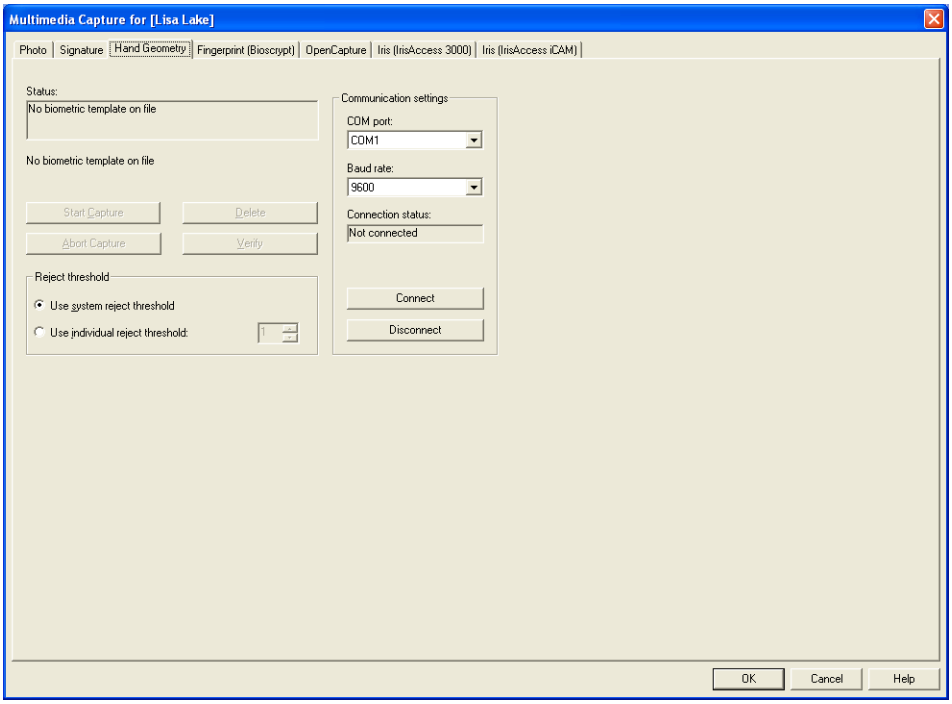
To use Hand Geometry hardware for enrollment, a support license (SWG-1400) and biometrics capture permissions are required. A user's capture permissions are set on the Cardholder Permission Groups form in the Users folder. For more information, refer to Cardholder Permission Groups Form on page 364.

HandKey Functionality

The HandKey readers capture three-dimensional images (templates) of a cardholder's hand. To do this, hand readers record 96 measurements including length, width and height of the fingers. These measurements are converted by mathematical algorithms into a 9-byte template.

The template of the cardholder's hand print is stored on the controller. When a badge or pin is presented to a reader, the controller downloads the template to the reader. The cardholder is then prompted to present his or her hand to the hand print reader for verification. The reader compares the stored template(s) with the cardholder's actual hand print. If the cardholder's hand print matches the template, the controller grants the cardholder access.

The HandKey reader is the only biometric reader supported by OnGuard that sends the biometric score data to Alarm Monitoring. If the Alarm Monitoring alarm filter includes biometric events and the column configuration includes biometric score, the following alarms will display in Alarm Monitoring: accepted biometric score, access granted or rejected biometric score, and biometric mismatch.



Status

Displays the status of the enrollment/capture process and prompts the user for specific action.

Start Capture

Initiates the capture procedure.

Abort Capture

Terminates the capture procedure. This button is only enabled when a hand print is being captured.

Delete

Deletes the displayed template.

Verify

Compares the live template with the stored template. The result of the comparison, the score, displays in the status field. The greater the difference between the two templates, the greater the score.

In segmented systems, default minimum scores required to accept a template match are set on the Biometrics sub-tab of the Segments form in the Segments folder. In non-segmented systems, default minimum scores are set on the Biometrics form in the System Options folder.

Use system reject threshold

Uses the administrator-defined minimum score required for biometric verification.

In segmented systems, administrators define this value on the Biometrics sub-tab of the Segments form in the Segments folder. In non-segmented systems administrators define this value on the Biometrics form in the System Options folder

Use individual reject threshold

Uses the minimum score you enter to determine hand print verification. Scores range from 1-255. The higher the value the better the hand to template match.

COM Port

Choose the number of the port that will be used to communicate with the hand reader.

Baud Rate

Enter the speed (in bits per second) at which information is transferred between the workstation and the hand reader.

Connection Status

Displays the connection status of the hand geometry reader. When the system tries to connect to the reader using the stored COM Port and Baud Rate settings, this field will display whether or not the reader is connected

Connect

Connects the hand geometry reader to the OnGuard system.

Disconnect

Disconnects the hand geometry reader from the OnGuard system.

Hand Geometry Procedures

The following procedures can be performed on this form.

Capture Hand Print Templates

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Hand Geometry tab.
3. Verify the reader is connected to the workstation. If not, click [Connect].
4. Verify the Communication settings (COM port and Baud rate) are correct.
5. If you want to use the system's rejection threshold, select the **Use system reject threshold** radio button. If you want to override the system's rejection threshold with an individual threshold value, select the **Use individual reject threshold** radio button and enter a value.
6. Click [Start Capture].
7. The status box in the Hand Geometry form provides instructions. Place your hand on the reader then remove it. The reader prompts you to do this three times in order to get a more accurate reading of your hand.
8. Once the template capture is complete, click [OK]. The Hand Geometry Form closes. Click [OK] on the Cardholders Form to end the process.

Note: When placing your hand on the Hand Geometry reader you must make sure to align your hand to the device. Light indicators will tell you your hand is being read. The lights will stay on if the device cannot read your hand geometry.

Verify Hand Print Templates

To verify that the user's hand geometry matches what is on record:

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.

2. Click the Hand Geometry tab.
3. Verify the reader is connected to the workstation. If not, click [Connect].
4. Verify the Communication settings (COM port and Baud rate) are correct.
5. Click [Verify].
6. You are asked to place your hand in the reader. After doing so, a number will appear in the status box. The lower the number the more likely the person verified is the same person whose hand was originally read.

Modify Hand Print Templates

Since you cannot modify someone's hand print template. The only way to modify what you have on record is to recapture the hand print template. To do this delete the record on the Hand Geometry form and repeat the capture process.

About Fingerprints

Every fingerprint is considered unique because of its pattern of ridges (raised skin) and furrows (lowered skin).

When you enroll a cardholder, you capture an image of their fingerprint as well as create and store a fingerprint template.

Fingerprint Images

A *fingerprint image* is a picture of a fingerprint.

With some biometric readers, you can store fingerprint images in the database when you enroll cardholders. Often this is not desirable for security reasons.

Fingerprint Templates

A *fingerprint template* is a series of points (minutiae points), that define fingerprint patterns. A fingerprint template is useless without a live image to compare it to. For this reason, storing fingerprint templates on smart cards, readers or controllers does not pose a security threat.

How Fingerprint Enrollment and Verification Works

Multimedia Capture and biometric hardware is used to capture a template of a cardholder's fingerprint. Depending on the type of hardware used, the template is stored either on a card, controller, or reader.

When a badge or pin number is presented to a reader, the cardholder is prompted to present his or her finger to a fingerprint reader for verification. The system then compares the stored template(s) with the cardholder's actual fingerprint. If the cardholder's fingerprint matches the stored template, the cardholder is granted access.

Fingerprint (Bioscrypt) Form

OnGuard supports the following Bioscrypt products:

- V-Smart - fingerprint and smart card (MIFARE or iCLASS) reader
- V-Flex - fingerprint reader that works in conjunction with any type of access control reader
- V-Station - fingerprint and PIN reader that works in conjunction with any type of access control reader
- MV-1200 - OEM module used with the LNL-BIO007-xxx
- V-Prox - fingerprint and proximity card reader
- V-Pass - standalone fingerprint reader

Fingerprint (Bioscrypt) License and Permissions

To use Bioscrypt hardware for enrollment, a support license (SWG-1402) and biometric capture permissions are required. A user's capture permissions are set on the Cardholder Permission Groups form in the Users folder. For more information, refer to Cardholder Permission Groups Form on page 364.

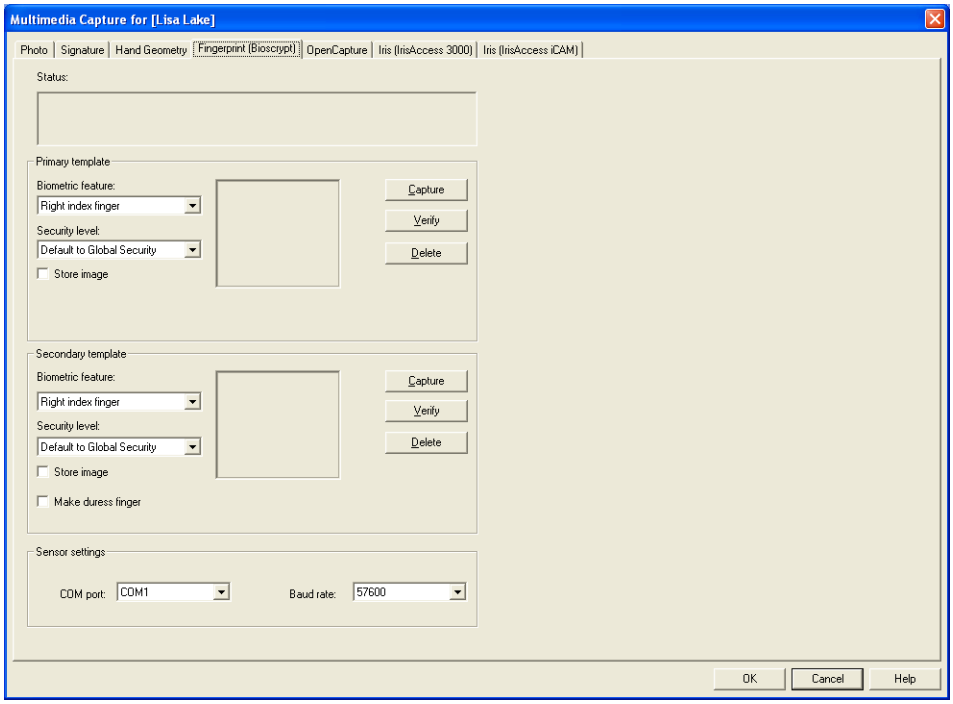
Bioscrypt Functionality

Bioscrypt hardware stores two fingerprint templates (primary and secondary) on the controller or smart card, depending on the type of hardware.

Secondary templates are added the same way primary templates are.

Note: Secondary templates are optional unless you use them for duress fingerprints or in the verification process if the primary template verification fails.

Additionally, before capturing an image, you can store fingerprint images in the database by selecting the **Store image** check box or you can designate the secondary fingerprint as duress by selecting the **Make duress finger** check box.



Status
Displays the fingerprint capture/enrollment status and prompts the user for specific action.

Fingerprint window
Displays the live image of the finger that is currently placed on the fingerprint sensor.

Biometric feature
Select which biometric feature you are capturing.

Security level
Select the security level which identifies the level of accuracy acceptable for template verification.

"Default to Global Security" uses the default system level set in the System Options folder (for non-segmented systems) or the Segments folder (segmented systems). The level you set here may be overridden, depending on the system default settings. For more information refer to the Biometrics form in the System Options or Segments folder.

Store image
Stores the image in the database. You must select this check box prior to capturing the fingerprint template.

Make duress finger
Specifies the second finger is designated as a duress finger. When that finger is presented, the system reports events as duress rather than normal.

Capture
Captures and displays the live image in the fingerprint window. If the **Store image** check box is selected prior to clicking [Capture], the image is also saved in the database.

Verify
Compares the live image with the stored template. The result of the comparison, whether the cardholder was verified or not, displays in the status window.

Delete
Deletes the selected fingerprint template.

COM Port
Choose the number of the port that will be used to communicate with the fingerprint reader.

Baud rate
Enter the speed (in bits per second) at which information is transferred between the workstation and the fingerprint reader.

Fingerprint (Bioscrypt) Procedures

The following procedures can be performed on this form.

Capture Fingerprint (Bioscrypt) Templates

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.

2. Click the Fingerprint (Bioscrypt) tab.
3. In the Sensor settings section, set up your workstation communication parameters.
   a. Select the COM port.
   b. Select the baud rate. This rate must match the baud rate configured at the enrollment Bioscrypt reader.
4. In the Settings section:
   a. Select the **Store image** check box if you want to store the fingerprint image in the database as well as view it in the Cardholders folder. The image is automatically sent to the controller through the workstation's Communication Server.
   b. Select the security level. "Default to Global Security" use the default system level.

Note: The level you set here may be overridden if your system is configured to use the default security level.

5. In the Fingerprint template sections:
   a. Select the biometric features to capture.
   b. To capture fingerprints using the duress option:
      - In the Secondary template section, select the finger you want to use as the duress finger. The Primary fingerprint is then used as the standard, non-duress fingerprint.
      - Select the **Make duress finger** check box. When a Bioscrypt fingerprint is captured, if the second fingerprint is specified as duress, the "Access Granted - Duress" event is reported when the duress finger is presented.
   c. Click [Capture] and place your finger on the biometric reader.
   d. Look at the Status field. If it states that a high quality and high content biometric template was captured, you are ready to verify the biometric capture. Otherwise, click [Delete] and recapture the fingerprint.
6. Click [OK].

Verify Fingerprint (Bioscrypt) Templates

Verifying the fingerprint template during the enrollment process prevents headaches later on. The verification process occurs after the fingerprint template is captured.

To verify the quality and content of the fingerprint template, click [Verify] (in Multimedia Capture) and refer to the status field for further instruction. The status field prompts the cardholder to place their finger on the reader as well as displays results of the verification process. If the fingerprint matches the template, the cardholder is identified/verified. Click [OK] when you are finished.

If you are working with V-Smart G or H hardware, you need to encode your smart card after you verify the quality and content of the fingerprint template.

Duress Fingerprint (Bioscrypt) Template

Normally, Bioscrypt hardware stores two fingerprint templates (primary and secondary) on the controller or smart card, depending on the type of hardware. For duress, the primary fingerprint template is presented as the standard (normal) fingerprint and the secondary as the duress fingerprint.

When a Bioscrypt fingerprint is captured, and the second fingerprint template is configured as secondary, normal access is granted if the second finger is presented. When the second fingerprint template is configured for duress, duress access is granted if the second finger is presented.

Encode Smart Cards with Bioscrypt Templates

For more information on encoding, refer to “Encoding Prerequisites” in the Workstations Folder chapter, Card formats Folder chapter, or Badge Types Folder chapter. The same information is available in each of these chapters.

Notes: When you position the card near the encoder, make sure to hold the card steady and within one inch of the encoder. If you encounter problems encoding, reposition the way you hold the card in front of the encoder.

The card format settings **Reversed Bit Order** and **Duress** are ignored when badges are encoded. For more information, refer to Wiegand Card Format Form on page 252 or Magnetic Card Format Form on page 248.

1. With the Cardholder form displayed click [Encode]. You may have to click [OK] before you can see the encode button.
2. The Encode Badge window opens. Select the Bioscrypt card format and the V-Smart (iCLASS) or V-Smart (MIFARE) encoder.
3. Click [Encode].
4. When prompted, present your card to the encoder.
5. When OnGuard displays the message that the encoding process was successful, click [OK]. If you get an error message, encode the card again. Make sure to review the tips at the beginning of this procedure.

OpenCapture Form

The OpenCapture line of physical security fingerprint readers supported by OnGuard is limited to the following devices:

- Cross Match ID 500 Fingerprint Scanner
- Cross Match Verifier 300 Fingerprint Scanner
- Sagem Morpho Smart Optical Fingerprint Scanners

Note: Refer to the OEM Device Configuration Guide for information on hardware installation.

OpenCapture Licenses and Permissions

To use OpenCapture for enrollment, a support license and biometrics capture permissions are required. A user’s capture permissions are set on the Cardholder Permission Groups form in the Users folder. For more information, refer to the Users Folder chapter in the System Administration User Guide.

Hardware support for the Cross Match ID 500, Cross Match Verifier 300, and Sagem Morpho Optical scanners are licensed features. Contact your Lenel representative for more information.

OpenCapture Functionality

Depending on which OpenCapture fingerprint scanner is used, the functionality of OpenCapture varies as follows:

- For the Cross Match ID 500: Capable of scanning multiple fingers at a time (4): Left Slap fingers, Right Slap fingers, and Double Thumb slap. The captured fingerprint images will store one set (ten individual prints) of finger data per enrollee. The Cross Match ID 500 scans fingerprint images only which are captured at 500 *ppi* (pixels per inch).
- For the Cross Match Verifier 300: Capable of scanning one finger at a time. Captures fingerprint images with vertical and horizontal resolutions of 500 ppi. The Verifier 300 fingerprint scanner is only capable of capturing a “flat” or “slap” image of a finger. It does not capture “roll” images.

Notes: OnGuard supports slap images, only.

Primary and secondary fingerprints captured using the Cross Match ID 500 or the Cross Match Verifier 300 are stored in the OnGuard database as ANSI-INCITS 378 minutiae templates.

- For the Sagem Morpho Smart Optical scanners: Capable of scanning one finger at a time. Captures fingerprint images with vertical and horizontal resolutions of 500 ppi. The MSO fingerprint scanner is only capable of capturing a “flat” or “slap” image of a finger. It does not capture “roll” images.

Note: Primary and secondary fingerprints captured with the Sagem MSO scanners are stored in the OnGuard database in two formats, Sagem Morpho PK_COMP v2 and ANSI-INCITS 378 minutiae templates.

OnGuard supports five models of the Sagem MSO scanners:

MSO 300. Provides images of 500 ppi with a larger form factor unit giving 416 x 416 pixel images.

MSO 350. Provides images of 500 ppi with a larger form factor unit giving 416 x 416 pixel images. Has an integrated contact PC/SC card reader.

MSO 350 PIV. Provides images of 500 ppi with a larger form factor unit giving 416 x 416 pixel images. Has an integrated contact PC/SC smart card reader which is approved for PIV applications. For more information, refer to PIV Card on page 102.

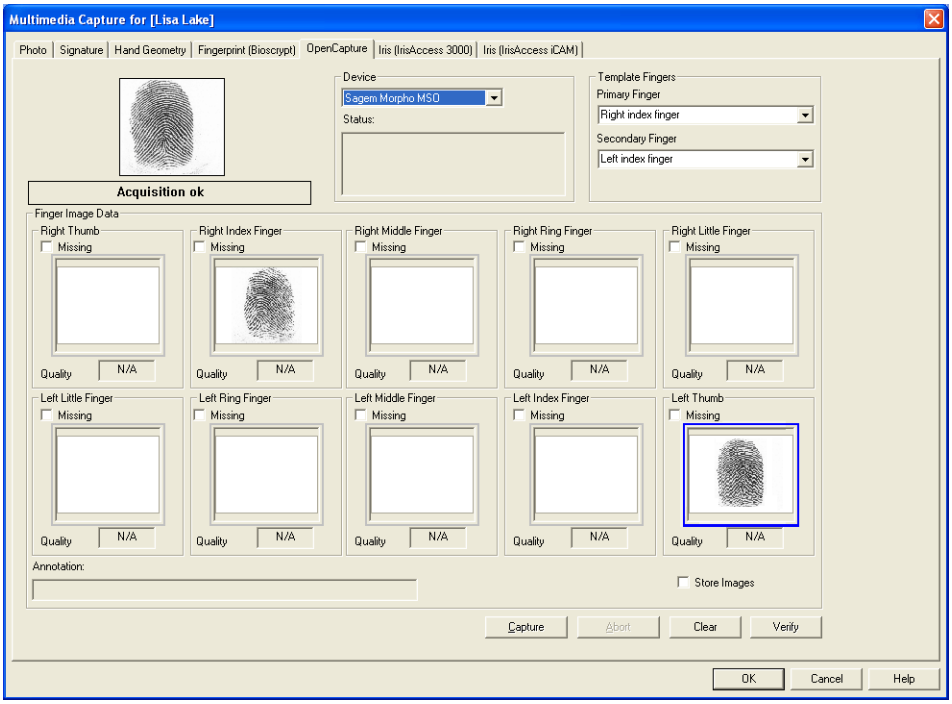
MSO 1300. Equivalent to the MSO 300 but at a smaller form factor and lower cost point than the MSO 300.

MSO 1350. Equivalent to MSO 350 but at a smaller form factor and lower cost than the MSO 350. Retains integrated smart card reader.

Fingerprint Verification

Primary and secondary fingerprints which are captured and saved in the template formats may be verified. The cardholder presents a finger on the scanner and the live fingerprint image is compared to the saved fingerprint template. If these match, verification is successful.

Note: Fingerprint verification is performed twice. The cardholder presents the same finger to the scanner to be verified first against the fingerprints stored in the Sagem Morpho PK_COMP v2 template and then against the ANSI-INCITS 378 minutiae template.



Live image

At the upper left of the form, the live fingerprint image is displayed as it is being captured if the device supports it. Device status is reported below the live fingerprint display.

Device

Select the device used to capture the fingerprint.

Status

Displays the current status of the scanning process, any messages, or instructions.

Primary Finger, Secondary Finger

Select a finger/thumb from the **Primary Finger** and **Secondary Finger** drop-down lists. When capturing a fingerprint specified as the **Primary Finger** or **Secondary Finger**, you must also select the corresponding finger/thumb group box. For example, if “Right Index” is selected for the **Primary Finger**, select the Right Index Finger group box as well.

For encoding DESFire (TWIC 1.02 Data Model) smart cards, both the right and left index fingerprints are required. To capture the right index fingerprint, the Right Index Finger group box and **Store Images** check box must be selected.
To capture the left index finger, the Left Index Finger group box and **Store Images** check box must be selected.

Primary and secondary fingerprints are also used for encoding other smart cards such as PIV cards.

Missing

Select if the cardholder has that particular finger/thumb missing.

Finger Image Data

Contains the finger/thumb group boxes. Each box displays the captured fingerprint image for the individual finger data. Before capturing a fingerprint, select the finger/thumb group box associated with the finger/thumb print you wish to capture.

Quality

Measures the quality of the capture. A high quality image is at least 60. **Quality** is only applicable to the Cross Match ID 500 scanner. For other scanners, "N/A" is displayed.

Annotation

Add notes (up to 128 characters) here for individual fingerprints. For example, a note might be added to indicate that an injury prevented the capture of the left index finger.

Store Images

Select to enable the saving of fingerprint images for the cardholder. To prevent casual database observers from looking at the raw fingerprint data it is stored as encrypted data in the database. The option to disable fingerprint storage is provided for organizations that do not wish to store fingerprint images for security and privacy considerations.

• WARNING! • A 416 x 416, 8-bit per pixel image is stored for each fingerprint in the fingerprint record for the cardholder. For example: If two (2) prints are captured for the cardholder, approximately 338 KB of disk space is required for the fingerprint record. However, if all 10 prints are saved in the fingerprint record, approximately 1.7 MB of disk space is required. Additionally, due to the size of such a fingerprint record, it may take a long time to save it over a WAN system. Therefore it is suggested that the enrollment workstation be connected via a high speed connection to the database server.

[Capture]

Click to begin the capture process.

[Abort]

Click to cancel the capture process.

[Clear]

Click to clear the finger/thumb print image and its associated information. If no finger is selected, all fingerprint images will be cleared. Before the image data is cleared, a prompt is displayed to confirm that the data is about to be deleted. Clearing all fingers will also delete the fingerprint templates from the database.

[Verify]

Click to perform fingerprint verification. The [Verify] button is enabled if you select a finger/thumb group box which corresponds to the selection in **Primary Finger** or **Secondary Finger**.

OpenCapture Procedures

The following procedures can be performed on this form.

Installation instructions for the fingerprint enrollment scanner devices are provided in the OEM Device Configuration Guide.

Capture Multiple Fingers

1. When enrolling a cardholder, click [Capture]. For more information, refer to Open Multimedia Capture on page 1343.
2. From the OpenCapture tab:
   a. Select the fingerprint scanner you are using from the **Device** drop-down.
   b. Check that the device status indicates it is connected. If this is not indicated, check your connection.
   c. If required, select a finger/thumb for the **Primary Finger** and **Secondary Finger**.
   d. If there are any fingers NOT being enrolled, select the **Missing** check box for that finger.

Note: Do NOT select any of the finger/thumb group boxes.

   e. Click [Capture]. Follow the on-screen prompts provided in the Status display. It will guide you through the process of capturing fingerprints and the using correct finger positions. First the right hand is captured, then the left hand, and last, both thumbs.
   f. If you wish to add an annotation for individual fingerprints, select the finger/thumb group box and type the information (up to 128 characters of data per finger).
   g. To verify the fingerprints, click [Verify]. For more information, refer to Verify Fingerprint Templates on page 1391.
   h. Click [OK] when you are done.

Capture Individual Finger

This procedure is used for scanners which capture a single finger at a time or if you need to re-scan a single finger during a multiple finger capture.

1. When enrolling a cardholder, click [Capture]. For more information, refer to Open Multimedia Capture on page 1343.
2. From the OpenCapture tab:
   a. Select the fingerprint scanner you are using from the **Device** drop-down.
   b. Ensure the device is connected. If this is not indicated, check the connection from the scanner to the workstation.
   c. If required, select a finger/thumb for the **Primary Finger** and **Secondary Finger**.
   d. Select the finger/thumb group box you will scan. A blue box is displayed around the selected group box.
   e. Click [Capture] to begin the capture process. Follow the on-screen prompts provided in the Status display. It will guide you through the process of capturing the fingerprint(s).
   f. Have the cardholder place a finger on the sensor. The cardholder will be prompted to do this a number of times to ensure a quality print is captured.
   g. Add an annotation for individual fingerprint(s) if you wish (up to 128 characters of data per finger).
   h. To verify the fingerprints, click [Verify]. For more information, refer to Verify Fingerprint Templates on page 1391.
   i. Click [OK] when you are done.

Verify Fingerprint Templates

1. From the OpenCapture tab, select the group box which corresponds to the finger/thumb specified for the **Primary Finger** or **Secondary Finger**.

2. Click [Verify]. Follow the on-screen prompts provided in the Status display.
3. The cardholder is prompted to place a finger on the sensor. The cardholder will be prompted to this a number of times.

Note: If a PK_COMP fingerprint template is present for the specified finger, the live fingerprint is tested against this template first and then the 378 minutiae fingerprint template.

4. When the verification is complete, click [OK] to close the OpenCapture form.

About Iris Patterns

The *iris* is the colorful portion of your eye that surrounds the pupil. Each iris is unique because it contains patterns such as collarettes, ciliary areas, pupilary areas, radial furrows, pigment frills and crypts.

Minutiae point algorithms capture this uniqueness by locating ridge bifurcations (where ridges join) and terminations (where ridges end) and mapping them numerically onto an iris template.

Iris (IrisAccess 3000) Form

The IrisAccess line of physical security iris readers supported by OnGuard include the ROU3000 (Remote Optical Unit) and the EOU3000 (Enrollment Optical Unit). In addition, the ICU3000 (Identification Control Unit) and extra boards are required for enrollment and access control.

License and Permissions

You do not need a special support license to use the IrisAccess 3000 hardware for enrollment or access control. The IrisAccess (iCLASS) application is licensed by the number of cardholders who have their irises captured.

However, biometrics capture permissions are required. A user's capture permissions are set on the Cardholder Permission Groups form in the Users folder.

Functionality

IrisAccess 3000 enrollment readers (EOU3000) do not store iris images or iris data. Instead, they send iris images to the ICU3000 where they are converted to 512-byte IrisCode. Then, using an HID (iCLASS) encoder, you can encode iCLASS smart cards with the iris data. IrisCode can also be encrypted prior to storing it to the smart card, using AES, DES or DES3 encryption methods.

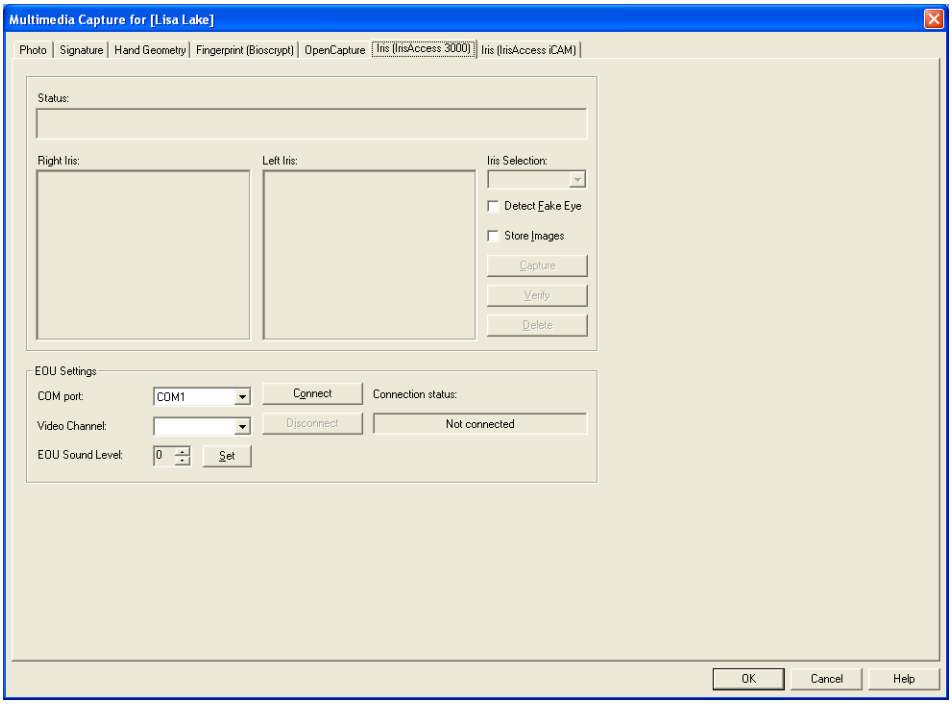
OnGuard can optionally store iris images in the database. IrisCode is not stored in the OnGuard application.

Enrollment Process

During the enrollment process, iris data is stored in a biometric container on smart cards. The biometric container is a part of the Lenel Open Card initiative. The system utilizes data from two applications stored on the card: access control data and the biometric container. Access control data can either be HID Access Control (iCLASS) data or IrisAccess (iCLASS) data.

Verification Process

1. An iCLASS card, with an HID Access Control application and biometric container, is presented to an HID iCLASS reader.
2. The reader (RW400) reads the access control data on the card and sends it up to the ICU.
3. The arrival of Wiegand data prompts the ICU to read the biometric container on the card.
4. After iris data is read, the ICU communicates to EOU3000, and the EOU3000 prompts the user to present their iris for verification.
5. The live image is compared to iris templates retrieved from the card.
6. If biometric verification is successful, access is granted or denied based on the cardholder's access levels. If biometric verification fails, access is denied.



Status

Displays the status of the capture procedure, including whether a capture is completed or failed, the number of failed attempts, and the amount (%) of information captured. A high quality image is at least 60%

Right Iris / Left Iris

Displays the live image of the iris as it is scanned and captured. Right and left images appear in this order to simulate a face to face appearance, instead of displaying the left image on the left side and the right image on the right side.

Iris Selection

Select which eye you are capturing. Choices are "Right" and "Left".

Detect Fake Eye

Select this check box to utilize additional security against using fake eyes. When this check box is selected, OnGuard engages the fake eye detection mechanism during iris capture and verification.

Store Images
Select this check box to store graphic images in the OnGuard database.

Capture
Click this button to initiate the capture procedure. The system makes three attempts to capture iris data. The status field displays the number of failed attempts and whether the capture is completed or failed.

Verify
Click this button to compare the live template with the stored template. The result of the comparison, a percentage, is displayed in the status window. A high quality image is at least 60%.

Delete
Click this button to delete both iris templates.

COM port
Choose the COM port (1 through 4) that will be used to communicate with the EOU3000.

Video Channel
Choose the channel (1 through 4) that the EOU3000 is connected to on the workstation's PC.

EOU Sound Level
The volume of the voice prompts and messages. Volume ranges from 0 to 8 (loudest).

Set
Click this button to set the volume of voice prompts and messages.

Connect
Click this button to connect the workstation to the EOU3000. The Connection status field displays "Connected" if a connection is established. Otherwise, "Not connected" displays in the Connection status field.

Disconnect
Click this button to disconnect the workstation from the EOU3000.

Connection status
Displays the connection status of the EOU3000.

OK
Saves your changes and closes Multimedia Capture. Don't forget to also click [OK] on the Cardholder form to save the biometric information.

Cancel
Closes the window and returns you to the Cardholder, Badge, or Access Levels form. Does not save any changes made in Multimedia Capture.

Help
Displays online help for this form.

Iris (IrisAccess 3000) Procedures

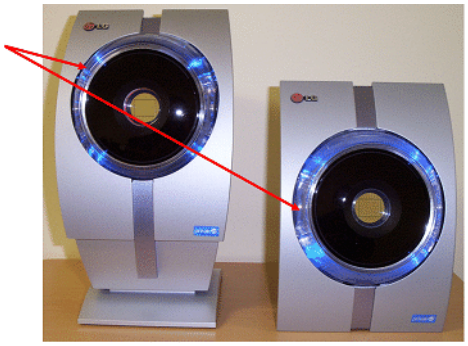
The following procedures can be performed on this form.

Capture Tips

- Although iris images can be captured through contact lenses, glasses, protective shields, and masks, it is highly recommended that cardholders remove their glasses, shields, or masks during enrollment. Cardholders do not need to remove contact lenses unless they have printed pattern contacts. Contact lenses, glasses, shields, and masks can be worn for enrollment verification and future readings.
- Inform cardholders that no lasers or bright lights are used to illuminate their eyes. Instead, a low level infrared light ray is used. The intensity of the ray is similar to rays used in a wireless television remote.
- Ask cardholders to sit down. There is less variance and movement during the capture process if the cardholder views the reader while seated.
- Ask cardholders to look into the reader from a distance of 3 to 10 inches (76.2 to 254 mm).
- Instruct cardholders to open their eye as wide as possible.
- When setting up the capture station, avoid bright lights in front or behind the reader.
- Take advantage of the visual signals on the reader that communicate its status.

Solid blue light - means the unit is on

Solid white/clear light - means the unit is off



Blinking green light - means the unit is capturing an image

Solid green light - means the image is accepted

Blinking red light - means the unit is inactive

Solid red - image rejected

Capture IrisAccess Templates

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Iris (IrisAccess 3000) tab.
3. Verify the EOU3000 reader is connected. If not, click [Connect].

4. Verify the EOU settings (COM port, video channel, and EOU sound level) are correct.
5. If you want to store the fingerprint image in the OnGuard database, select the **Store image** check box.
6. For additional security, select the **Detect Fake Eye** check box.
7. Select which eye you are enrolling (left or right), from the **Iris Selection** drop-down list.
8. Ask the cardholder to look into the enrollment reader. Cardholders should position themselves 3 to 10 inches (76.2 to 254 mm) away from the reader.
9. While the cardholder is looking into the reader, click [Capture].

Note: Verbal commands let the cardholder know if they are too close or too far from the reader.

10. The status field identifies the capture quality. If the template is high quality (60% or greater) repeat the capture process for the other eye. If only one eye is available, you should capture that eye twice. If the template is low quality, recapture an image of the same eye.

Verify IrisAccess Templates

Verifying iris templates during the enrollment process prevents headaches later on. The verification process occurs after the iris image is captured.

To verify the quality and content of the iris image, click [Verify] (in Multimedia Capture). The reader prompts the cardholder to look into the reader. If the iris pattern matches the template, the reader announces that the cardholder is identified/verified.

Note: It is not necessary to select which eye you are verifying. During verification, the system will search through all of the cardholder's iris templates for a match.

Encode Smart Cards with IrisAccess Templates and Access Control Information

For more information on encoding, refer to "Encoding Prerequisites" in the Workstations Folder chapter, Card formats Folder chapter, or Badge Types Folder chapter. The same information is available in each of these chapters.

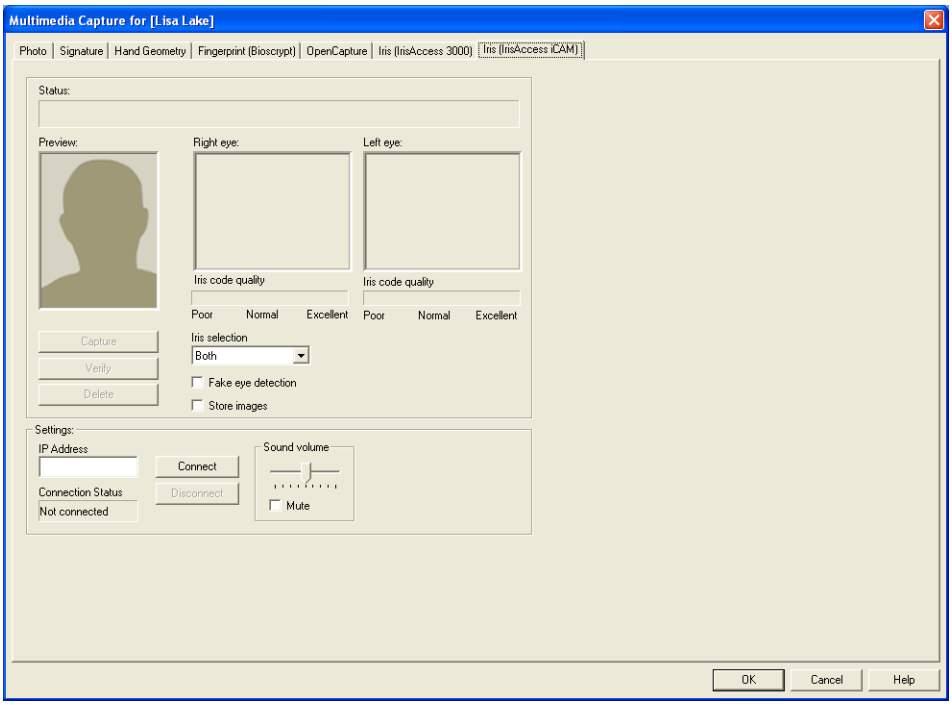
Note: When you place the card near the encoder be sure to keep the card steady and within 1 inch (2.54 cm) of the encoder. If you encounter problems encoding, reposition the way you hold the card in front of the encoder.

1. With the Cardholder form displayed click [Encode].
2. The Encode Badge window opens. Select the HID (iCLASS) smart card format and HID (iCLASS) encoder to encode the cardholder's access control data.
3. Click [Encode].
4. When prompted, present your card to the HID iCLASS encoder and click [OK].
5. When OnGuard displays the message that the encoding process was successful, click [OK]. If you get an error message, encode the card again.
6. In the Cardholder form, click [Encode].
7. The Encode Badge window opens. This time, select the Iris Access (iCLASS) card format and HID iCLASS encoder.
8. When prompted, present your card to the HID iCLASS encoder and click [OK].

9. When OnGuard displays the message that the encoding process was successful, click [OK]. If you get an error message, repeat steps 6-8.

Iris (IrisAccess iCAM) Form

Note: Two workstations cannot be connected to iCAM network devices at the same time.



Status

Displays the status of the capture procedure, including whether a capture is completed or failed, the number of failed attempts, and the amount (%) of information captured. A high quality image is at least 60%.

Preview

Displays the live preview of the camera.

Right eye/ Left eye

Displays the live image of the eye as it is scanned and captured. The field below each eye show the quality of the capture. Right and left images appear in this order to simulate a face to face appearance, instead of displaying the left image on the left side and the right image on the right side.

Iris Selection

Select which eye you are capturing. Choices are “Right”, “Left”, and “Both”.

Fake eye detection

Select this check box to utilize additional security against using fake eyes. When this check box is selected, OnGuard engages the fake eye detection mechanism during iris capture and verification.

Store Images
Select this check box to store graphic images in the OnGuard database.

Capture
Click this button to initiate the capture procedure. The status field displays “Capture successful”' and the voice on the reader informs you when the procedure is finished.

Verify
Click this button to compare the live template with the stored template. The result of the comparison, a percentage, is displayed in the status window. A high quality image is at least 60%.

Delete
Click this button to delete both iris templates.

IP Address
Enter the IP address you used during the setup the Iris (IrisAccess iCAM) ICU controller and camera.

Connection Status
Displays current connection status of the IrisAccess iCAM.

Connect
Click this button to connect the workstation. The Connection status field displays “Connected” if a connection is established. Otherwise, “Connection failed” displays in the Connection status field.

Disconnect
Click this button to disconnect the workstation.

Sound volume
Regulates the volume of the voice prompts and messages.

Mute
Mutes the sound from the reader.

OK
Saves your changes and closes Multimedia Capture. Don’t forget to also click [OK] on the Cardholder form to save the biometric information.

Cancel
Closes the window and returns you to the Cardholder, Badge, or Access Levels form. Does not save any changes made in Multimedia Capture.

Help
Displays online help for this form.

Capture IrisAccess Templates

1. Open Multimedia Capture. For more information, refer to Open Multimedia Capture on page 1343.
2. Click the Iris (IrisAccess iCAM) tab.

3. Verify the reader is connected. If not, enter the IP address and click [Connect].
4. If you want to store the fingerprint image in the OnGuard database, select the **Store image** check box.
5. For additional security, select the **Detect Fake Eye** check box.
6. Select which eye you are enrolling (left, right, or both), from the **Iris Selection** drop-down list.
7. Ask the cardholder to look into the enrollment reader. Cardholders should position themselves 3 to 10 inches (76.2 to 254 mm) away from the reader.
8. While the cardholder is looking into the reader, click [Capture].

Note: Verbal commands let the cardholder know if they are too close or too far from the reader.

9. The status field identifies the capture quality. If the template is high quality (60% or greater) repeat the capture process for the other eye. If only one eye is available, you should capture that eye twice. If the template is low quality, recapture an image of the same eye.

Verify IrisAccess Templates

Verifying iris templates during the enrollment process prevents headaches later on. The verification process occurs after the iris image is captured.

To verify the quality and content of the iris image, click [Verify] (in Multimedia Capture). Select which eye you are verifying, (left, right, or both) from the **Iris Selection** drop-down list. The reader prompts the cardholder to look into the reader. If the iris pattern matches the template, the reader announces that the cardholder is identified/verified.

Encode Smart Cards with IrisAccess Templates and Access Control Information

For more information on encoding, refer to “Encoding Prerequisites” in the Workstations Folder chapter, Card formats Folder chapter, or Badge Types Folder chapter. The same information is available in each of these chapters.

Note: When you place the card near the encoder be sure to keep the card steady and within 1 inch (2.54 cm) of the encoder. If you encounter problems encoding, reposition the way you hold the card in front of the encoder.

1. With the Cardholder form displayed click [Encode].
2. The Encode Badge window opens. Select the HID (iCLASS) smart card format and HID (iCLASS) encoder to encode the cardholder’s access control data.
3. Click [Encode].
4. When prompted, present your card to the HID iCLASS encoder and click [OK].
5. When OnGuard displays the message that the encoding process was successful, click [OK]. If you get an error message, encode the card again.
6. In the Cardholder form, click [Encode].
7. The Encode Badge window opens. This time, select the IrisAccess (iCLASS) card format and HID iCLASS encoder.
8. When prompted, present your card to the HID iCLASS encoder and click [OK].

When OnGuard displays the message that the encoding process was successful, click [OK]. If you get an error message, repeat steps 6-8.

APPENDIX D

Reports

Reports are installed when Database Setup is run. All reports are installed on the database server under the ReportTemplates subdirectory in the OnGuard installation path. By default, this location is **C:\Program Files\OnGuard\ReportTemplates**.

Notes: For custom reports you must use the actual data field and not the internal database ID.

Refer to the release notes for the versions of Seagate Crystal Reports that are supported. The release notes are located on the root of the OnGuard installation disc.

Description of Reports

Access Denials and Grants, by Reader
Badge-related events, grouped by reader.

Access Denials, Grants and Other Badge Events
All badge-related events, including time, reader, badge and cardholder name. All badge events will be shown.

Access Denied Events
All Access Denied events, including time, reader, badge, and cardholder name.

Access Denied Events, by Reader
Access Denied Events, grouped by reader.

Access Granted Events
All Access Granted events, including time, reader, badge, and cardholder name.

Access Granted Events, by Reader
Access Granted events, grouped by reader.

Access Groups
Lists all Access Groups and the Access Levels contained in each group.

Access Groups With Levels
Access Group definitions including access level details.

Access Level Assignments to Cardholders
Listing of each Access Level, with each cardholder that has that access level assigned to them. Also summarizes the total number of badges that need to be downloaded.

Access Level Assignments to Cardholders, by Segment
Listing of each Access Level by Segment, with each cardholder that has that access level assigned to them. Also summarizes the total number of badges that need to be downloaded to each segment. This report is valid only for systems using Segmentation.

Access Levels
Access Level definitions.

Access Panels
Access Panel definitions.

Active Visits, by Host Name
Lists all visits that are currently active (not signed out), grouped by host name.

Active Visits, by Visitor Name
Lists all visits that are currently active (not signed out), grouped by visitor name.

Alarm Acknowledgments
All alarm acknowledgments, including the alarm information and acknowledgment notes.

Alarm Acknowledgments, by Definition
All alarm acknowledgments, grouped by alarm definition.

Alarm Acknowledgments, by Operator
All alarm acknowledgments, grouped by system operator.

Alarm Acknowledgments, by Panel
All alarm acknowledgments, grouped by panel.

Alarm Configuration
Alarm configuration summary.

Alarm Input Events
All alarm input events by date.

Alarm Panel Inputs
Lists all alarm panel inputs, grouped by main panel and alarm panel.

Alarm Panel Local Linkage
Lists alarm input/output local links on alarm panels.

Alarm Panel Outputs
Lists all alarm panel outputs, grouped by access panel and alarm panel.

Alarm Panels
Lists all alarm panels, grouped by parent panel.

All Cardholders With Logical Access
Lists all cardholders that have linked logical access accounts.

All Events Over Time
A listing of all event types over time.

All Events Over Time With Local Panel Time
Lists all event types over time. This report also shows the time an event occurred in the panel's time. This report might generate slowly.

All Events Over Time With NGP Area
A listing of all event types over time for NGP panels. This report also shows the area for intrusion-related events (Arm, Disarm, and so on).

All Events Over Time With Unique Alarm ID
A listing of all event types over time with unique alarm IDs.

All Events Over Time With Unique Alarm ID
A listing of all event types over time with their unique alarm IDs included. This report displays the selected event types that occurred over a specific time and the unique alarm ID associated with each event type.

Anti-Passback Events
All anti-passback events over time.

Area Configuration
Lists all areas, including the reader entrances and exits.

Area Entrance History
History of all cardholders entering areas, sorted by area and date.

Asset Classes
Lists all asset classes and the asset groups to which they belong.

Asset Events
All events having to do with assets.

Asset Groups
Lists all asset groups and the classes they contain.

Asset Types
Lists all defined asset types and their subtypes.

Assets, by Scan ID
Lists all assets, sorted by Scan ID.

Assets, by Type
Lists all assets, sorted by type and subtype.

Assigned Assets by Type, Scan ID
Lists all currently assigned assets, sorted by type and Scan ID.

Assigned Assets, by Cardholder
Lists all currently assigned assets, sorted by cardholder.

Assigned Assets, by Scan ID
Lists all currently assigned assets, sorted by Scan ID.

Audio Notifications and Instructions
Lists all audio notifications and instructions in the database.

Badge Type Configuration
Lists all badge types that have been configured in the system.

Badges Without Access Levels
Lists all badges with no assigned access levels.

Badges, by Deactivate Date
Listing of all badges by deactivate date. Can be used to determine which badges are about to expire.

Card Formats
Definitions of all Magnetic and Wiegand card formats in the system. This combined report replaces the Magnetic Card Formats and Wiegand Card Formats reports that were available with previous software releases.

Cardholder Access to Readers
Listing of each reader, and which cardholders have access to that reader. Includes the associated access level and timezone.

Cardholder Exit/Entry
Displays user-defined Exit/Entry on a per-cardholder basis. To run this report, readers must be designated as 'Time and Attendance' Entrance or Exit readers on the Readers/Controls page. This is not an Area report.

Cardholder Photo Gallery
All cardholder photos, sorted by name.

Cardholder Precision Access to Readers
Listing of each reader, and which cardholders have precision access to that reader. Includes the associated precision access and time zone.

Cardholder Time and Attendance
Pairs each in-time with an out-time for cardholders gaining entry to time and attendance readers.

Cardholders Located in Each Area, by Date
List of the cardholders located in each area, sorted by area and date.

Cardholders Located in Each Area, by Name
List of the cardholders located in each area, sorted by area and cardholder name.

Cardholders With Access, by Badge Type
All cardholders with active badges that have access, sorted by badge type. Includes access level assignments.

Cardholders With Access, by Last Name

All cardholders with active badges that have access, sorted by last name. Includes access level assignments.

Cardholders With Precision Access, by Badge Type

All cardholders with active badges that have access, sorted by badge type. Includes precision access level assignments.

Cardholders With Precision Access, by Last Name

All cardholders with active badges that have access, sorted by last name. Includes precision access level assignments.

Cardholders, by Badge Type

All cardholders sorted by badge type, no access levels shown.

Only personnel with badges assigned will be included in this report.

Cardholders, by Last Name

All cardholders sorted by last name, with badges but no access levels.

Only personnel with badges assigned will be included in this report.

CCTV Instructions

Summary of all CCTV instructions in the database.

Continuous Video

Lists all of the times that there has been continuous video archived.

Current Visits

Lists all currently signed in visits.

Destination Assurance Configuration

Lists all entrance readers, their settings, and the associated exit readers.

Destination Assurance Exempt Cardholders

Lists all cardholders who have a badge that is exempt from destination assurance.

Device Status Events

Status events for all devices.

Dialup Events, by Panel

Lists all dialup events, grouped by panel.

Dialup Last Connect Time

Lists online dialup panels, and the last time they were connected.

Elevator Access Denied and Granted Events

All Access Denied and Granted events for elevator readers with the Track Floors option enabled. Includes time, reader, badge, cardholder name, and the floor to which access was attempted. All access denials and grants are shown.

Elevator Dispatching Devices and Terminals

Lists all elevator dispatching devices with the configured terminals.

Elevator Floor Assignments to Cardholders
Lists all cardholders that have access to a particular elevator floor list.

Emergency Events
All emergency events over time.

Event Codes
Event code templates and event code mapping configuration.

Event Count, by Panel
A count of all events, grouped by panel. Includes a pie chart graphic of the event counts.

Fire Device Input/Outputs
Lists all fire input/outputs, grouped by panel and fire device.

Global Area/MobileVerify Occupancy, by Date
Shows the last known area accessed by each cardholder, sorted by date and time.

Global Area/MobileVerify Occupancy, by Name
Shows the last known area accessed by each cardholder, sorted by name.

Global I/O Linkages
Lists all of the global I/O linkages, including the input events and output actions.

Guard Tour Configuration
Lists all of the configured guard tours including checkpoints, actions, and messages.

Guard Tour History
Lists all of the events, associated with checkpoints, that happened for each guard tour.

Hardware Panels
Lists all top-level hardware panels by category, including access, fire, intercom, and personal safety.

Holidays
Lists all system holiday definitions.

ILS Lock Authorizations, by Cardholder
Lists ILS lock authorization levels assigned to the cardholder/badge, sorted by cardholder.

ILS Authorizations, by Level
Lists ILS lock authorization levels assigned to the cardholder/badge, sorted by level.

ILS Lock Battery Status, by Status
Lists ILS lock battery status, grouped by battery status (Low to High), wireless gateway, and battery percent.

ILS Lock Characteristics
Lists ILS lock configuration details, sorted by lock name.

ILS Lock Communications
Lists ILS wireless lock diagnostics, sorted by lock name.

ILS Lock Ownership
Lists the ILS locks owned by a cardholder.

Intercom Functions
Lists all defined intercom functions.

Intercom Stations
Lists all intercom stations, grouped by intercom exchange.

Intrusion Command Authority - Advanced
Lists all cardholders that have access level assignments configured to use advanced intrusion command authority.

Intrusion Command Authority - Global
Lists all cardholders who are assigned access levels with global intrusion command authority.

Intrusion Command Events
Lists all events associated with intrusion commands, including device, cardholder name, and badge.

Intrusion Detection Areas
Lists all intrusion areas grouped by panel.

Intrusion Detection Devices
Lists all of the intrusion detection devices grouped by panel.

Intrusion Panel User Groups
Lists all panel users grouped by panel user groups.

Last Location of Cardholders
Shows the last reader accessed by each cardholder, sorted by cardholder name.

Locked Video Events
Lists all system events with associated locked video events.

Maps
List of available maps in the database.

MobileVerify User Transaction Log
Chronological log of all transactions performed.

MobileVerify User Transaction Log, by Operation
Chronological log of all transactions performed, grouped by operation.

MobileVerify User Transaction Log, by User ID
Chronological log of all transactions performed, grouped by User ID.

Module Details
Lists all module definitions, grouped by parent panel.

Module Summary
Lists all modules, grouped by parent panel.

Monitor Stations

Lists all alarm monitoring stations defined in the system, including which monitor zones and access panels they are monitoring.

Monitor Zones

Lists all Monitoring Zone definitions.

NGP Central Station Setup

Lists, for use by the central station, the numerical reference (key) to the Areas, Zones (Points), and Access Doors configured within the NGP Panel. The central station uses this information when programming the central station automation system to correctly identify items reported from the NGP panel.

IMPORTANT: When you change the configuration of a system connected to central station reporting, re-run the Central Station Setup report to ensure it matches what is reported by the central station. Configuration changes that require this action include:

- Adding or deleting an alarm panel.
- Increasing or decreasing the number of alarm inputs allocated to an alarm panel.
- Adding or deleting a door.

NGP Panels

Lists all NGP panel definitions.

NGP User ID Report

Lists all cardholders that have NGP User ID assignments.

Overdue Visits

Lists all scheduled visits that have not signed in.

Overstayed Visits

Lists all visitors logged into the facility, but whose badge or visit has expired.

Permission Profiles

Lists all permission profile definitions.

Personal Safety Transmitter Assignments

Lists all assignments of personal safety transmitters to cardholders, assets, and so on.

Personal Safety Transmitters

Lists all personal safety transmitters.

Personnel Without an Active Badge

Lists all personnel in the database who do not have an active badge assigned to them.

Personnel, by Last Name

Lists all personnel in the database, with basic information only.

Personnel, Organization Details

Lists all personnel in the database, with organization details. This report is designed for the standard cardholder layout. It might not work with user-customized cardholder layouts.

Personnel, Personal Details
Lists all personnel in the database, with personal details. This report is designed for the standard cardholder and visitor layout. It might not work with user-customized cardholder and visitor layouts.

Point of Sale Registers
Lists all point of sale registers by point of sale device.

Precision Access Groups
Precision Access Group definitions.

Reader Assignments to Cardholders
Lists all cardholders that have access to a particular reader.

Reader Command Programming Configuration
Lists all command programming readers along with the associated user and instant commands.

Reader Precision Access Assignments to Cardholders
Lists all cardholders that have precision access to a particular reader.

Reader Status Events
All reader status events, grouped by reader.

Reader Timezone Schedules
Reader timezone scheduling for reader modes.

Readers
Reader definitions, grouped by access panel.

Receiver Account Alarm Activity
Lists all alarm activity for receiver accounts including notes and elapsed times.

Receiver Account Areas
Lists all receiver account areas, grouped by receiver account.

Receiver Account Groups
Lists all receiver account groups and the receiver accounts contained in each group.

Receiver Account Zones
Lists all receiver account zones, grouped by receiver account.

Receiver Accounts
Lists all receiver accounts.

Receiver Accounts That Failed to Report
Lists all of the receiver accounts that failed to report during their duration.

Receiver and Receiver Account Events
Lists all the events that occurred on a receiver or receiver account.

Segment Badge Download Summary
For each segment, lists the count of badges that must be downloaded to the access panels in that segment. This report is valid only for systems that use the Segmentation feature.

Segments
Lists all segments defined on the system and their options. This report is valid only for systems that use the Segmentation feature.

SNMP Agents
Lists all SNMP agents sorted by segment and name.

SNMP Management Information Base Configuration
Lists all MIB data, grouped by enterprise.

System Servers
Lists all servers defined on the system.

Text Instructions and Acknowledgment Notes
Lists all text instructions and acknowledgment notes.

Timezones
Lists all timezone definitions.

User Permissions
Lists all system users and their permissions.

User Transaction Log
Chronological log of all transactions performed on the system by users.

User Transaction Log, by User ID
Chronological log of all transactions performed on the system, grouped by User ID.

Users With Area Access Levels to Manage
Lists all Area Access Manager users and the access levels they manage.

Video Camera Device Links
Lists the device links for each camera.

Video Cameras
Lists all video cameras, grouped by video server.

Video Servers
Lists all video servers.

Visit History
History of all visits in the system.

Visit History With Host
History of all visitors that visited the facility with their host.

Visitors
Lists all visitors in the system.

This report might not run properly if you have deleted the default visitor fields using FormDesigner.

APPENDIX E

Segmentation

The Segmentation feature offers several significant advantages, including:

Extended Hardware Limitations. Access control hardware has limited memory. There is a limited amount of access levels, badges, access level assignments to badges, timezones, and other database components that the access control hardware can store. Segmentation provides a logical way to group hardware so that these limits exist only on a per-segment basis. For example, instead of having a maximum of six access levels per badge system-wide, a segmented system can have six access levels per segment per badge.

Ability to Manage User Access to the System. In a segmented system, users are assigned to one or more segments. All segmented objects in the system are filtered appropriately so that a user only sees objects that are in their segment(s) and objects that are system-wide. For example, a user might be granted administrative permissions, but only in one segment.

More Efficient Cardholder Downloads. In a segmented system, only badges that have access to a particular segment are downloaded to the hardware in that segment. This reduces hardware memory requirements for segments that do not require a high cardholder population. For example, a badge record is downloaded to access levels in a segment only if the badge record has at least one access level in that segment. Therefore, a segmented installation that has 30,000 cardholders does not necessarily need to have on each of its access panels the memory capacity for 30,000 cardholders.

Notes: For users with access to only one segment, OnGuard will behave essentially the same as it would in a non-segmented system (records they create will automatically be placed in their segment). Users who have access to multiple segments will need to specify which segment(s) a record belongs to.

Not all object types can be segmented. Objects that cannot be segmented are considered system-wide objects.

Segments and Segment Groups

A *segment* is the basic unit of segmentation, and is a “partition” or a “subset” of the entire OnGuard system. A segment provides various options that apply to any device that belongs in that segment.

When a segment is added to the system, a user can copy records and move devices from a source segment, providing an effective means for splitting an existing system into smaller, distinct segments.

A *segment group* is a simple collection of one or more segments. It is highly recommended that you use segment group assignments where possible, especially for users and cardholders. Using segment groups reduces management effort and complexity. For example, when a new segment is added to the system, the administrator simply adds it to the appropriate segment group and users and cardholders with those groups assigned are granted access to the new segment. A segment may belong to multiple segment groups. For example, one group may contain segments A and B, another group C and D, and another group segments A, B, C, and D. Currently, one segment group cannot contain another segment group.

Segment Rules and Multiple Segment Assignments

Users may be granted access to multiple segments via multiple segment assignments, a segment group assignment, or both.

Note: For ease of management in multiple segment cases, it is recommended that you use one or more segment group assignment rather than assign multiple individual segments to a user.

Some objects in the system can belong to multiple segments, by allowing the assignment of a segment group or multiple segment assignments.

The general rules of multiple segment assignments are:

- To view an object, the user must have access to one common segment of the object. For example, if a monitoring zone belongs to segment group ABC, a user with access only to segment A would be able to see the monitoring zone. However, the user would only be able to see the devices in the monitoring zone that belong to segment A.
- To edit an object, the user must have access to all the segments assigned to the object. For example, if a monitoring zone belongs to segment group ABC, a user assigned to segment group ABC or ABCD would be able to edit the object. However, a user assigned to segment group AB would not be able to edit the object.

Segment Users and <All Segments> Assignments

In a segmented system, there are two types of users, segment users and <All Segments> users. A segment user is restricted to working within one segment only. For segment users, the user interface differences between a non-segmented and a segmented system are negligible. The user's segment is added to the title bar, and for segmentable objects they will only see records that exist in their segment. When they add a record, it is automatically assigned to their segment if it is a segmentable object.

A segment user cannot:

- Add or delete segments. The person can modify only the segment to which he or she has been assigned.
- Perform transaction/event purging and archiving. Because purging is a system-wide process, only <All Segments> Users can do this.
- Log in to the FormsDesigner or BadgeDesigner applications.

<All Segments> is a special segment assignment that can be assigned to some object types. An <All Segments> assignment means system-wide access, regardless of how many segments are in the system. When assigned to a user, the user will always have access to any segment and any object in the system.

Note: A segment group that currently contains every segment in the system will not behave the same way as an <All Segments> assignment.

The general rules of <All Segments> assignments are:

- Any user can view an <All Segments> record; however, if the object contains assignments of other segmented objects, they can only view those that exist within their segments. For example, any user can see an access group that belongs to <All Segments>. However, the user can only see and assign the access level members of that group that are in segments to which they have access.
- Only users with <All Segments> access can add, modify, and delete records that are <All Segments>.

Note: Users that do not have <All Segments> access cannot view other users that do have <All Segments> access. This includes records related to those users, such as user transactions.

Primary Segments

The concept of a primary segment applies to the advanced segmentation options of segmenting badge types and cardholders and was introduced to allow more precise control over objects that can now belong to multiple segments. The primary segment assignment can be either an individual segment or a segment group.

The primary segment determines who can add, modify, and delete a badge of that type; a user only needs access to the primary segment of the badge type to do so. However, a user must have access to all segments that a badge type belongs to in order to modify or delete the badge type itself.

The primary segment determines which users can add, modify, and delete a cardholder, as well as edit any other assignment to the cardholder. A user only needs access to the primary segment of the cardholder to do so.

Notes: Although a primary segment is selected for card formats when they are segmented, it currently has no practical implications. A user only needs access to one of the card format's segments in order to assign it to a badge type or reader, and a user must have access to all segments assigned to a card format in order to edit it.

Users currently are not assigned a primary segment. However, a user must have access to all segments that a user record has in order to edit that record. This is consistent with the current rules that you cannot edit a user that has more access than you.

Advanced Segmentation

Choosing to segment an object affects its eligibility to be assigned to other objects, its eligibility to have other objects assigned to it, and a user's ability to view, assign, and edit the object. The following segmentation objects can optionally be enabled:

Segment Card Formats. This feature allows systems that require many different card formats to grow beyond the normal maximum number of card formats that can be stored in access control hardware. A card format can be system-wide, or belong to one or more segments. For each card format available in a segment, a unique hardware ID is maintained. A card format's segment membership filters the readers to which the format may be assigned, based on the segment of the reader's parent panel.

Segment Badges via Badge Types. Badge types can be segmented and badges are therefore segmented by nature of their type. Depending on other segment option settings, a badge type's segment membership can determine eligibility for card formats, access level assignments to badges, and badge type assignments to cardholders.

Segment Cardholders. A cardholder's segment assignment affects which users can view and edit the cardholder, which access levels can be assigned to the cardholder, and if the badge types are also segmented, which badge types can be assigned to the cardholder.

Segment Visitors. If cardholders are segmented, visitors can optionally be segmented as well. Segmenting visitors restricts which users can view and edit them, as well as which cardholders they can be assigned to visit.

Allow Segments to Belong to More than one Segment Group. This setting is enabled by default. It can be disabled to enforce a rule that a segment can belong to one and only one segment group.

Allow Access Levels to be Configured as Assignable by Users in Other Segments. This option is intended for tenant/landlord scenarios, allowing a landlord to designate a subset of access levels for common readers to be assignable by tenants without having to give tenants full access to the landlord segment.

Usage Scenarios

Many of the advanced segmentation features such as cardholder and badge type segmentation are intended for tenant/landlord scenarios. In such scenarios, a landlord organization runs one or more buildings that house tenants from different organizations. Depending on the situation, a landlord may wish to give tenants varying degrees of access and control into the OnGuard system, allowing flexibility in the level of services that can be provided to tenants without the need for direct landlord involvement.

The design of these features allows for a powerful and flexible approach to segmentation that can be utilized in many diverse scenarios, for example:

- A single company can choose to segment card formats only, to accommodate a large number of card formats and facility codes.
- A university can choose to segment only cardholders, while keeping common badge types and card formats, to manage user access to view and edit various groups of students and faculty.
- A large conglomerate can segment cardholders, badge types and formats, using different segments and segment groups for each company that is part of the conglomerate. This allows a central security organization to seamlessly manage a diverse set of companies. Segment filtering means that each company will only see their own employees, which not only restricts access but also filters out superfluous records. The flexibility of segmentation allows employees to belong to multiple segments and segment groups, making it easy to accommodate employees needing access to more than one company.

The following table shows some of the common combination of segmentation options and example applications. The table provides some possible applications; however, the needs of each system must

always be thoroughly evaluated when considering configuration options, so that the optimal solution is implemented in each case.

Card Formats	Badge Types, Badges	Cardholders	Visitors	Example Application
Yes	No	No	No	Simply allows for more card formats. Typically for a single organization needing many different card formats.
Yes/No	No	Yes	No	Single organization with common badge types and visitors. Cardholders are segmented in order to manage user access to cardholders and restrict cardholder access level eligibility. For example, a university might use segments to categorize faculty, students, and other people by school, dormitory, and other criteria.
Yes/No	Yes	Yes	No	Segmented badge types and cardholders, but common visitors that any user can see and can visit any cardholder. This could be used for: • A single organization that wishes to control user and cardholder access to various badge types. • A tenant/landlord situation where policy dictates that any tenant user is allowed to see any outside visitors enrolled in the system. Also allows simplified tracking of the same person visiting multiple tenants. **Note:** A tenant user would not be able to see visit records for other tenants even though they can view the same visitors.
Yes/No	No	Yes	Yes	Common badge types, but segmented cardholders and visitors. Could be used in a tenant/landlord situation where the landlord does not require the additional maintenance of segmented badge types for every tenant. A few common badge types with common layouts are used.
Yes/No	Yes	Yes	Yes	Full segmentation that is well suited to a fully featured tenant/landlord application.

Card Format Segmentation

When card format segmentation is enabled, a format can be assigned to <All Segments> (system-wide), or one or more individual segments. Access control hardware typically has a maximum number of card format IDs it supports. For example, anLNL-1000 access panel supports up to eight formats with IDs 1-8. Therefore, the system ensures that the next available unique hardware ID is assigned to a card format for each segment in which it belongs. For example, assume:

- An <All Segments> card format exists, using hardware ID 1 system-wide.
- Segment A has one card format with hardware ID 2.
- Segment B has two card formats, with hardware IDs 2 and 3.
- Segment C has three card formats, with hardware IDs 2, 3, and 5.

If a new card format is added and assigned to segments A, B, and C:

- Hardware ID 3 will be assigned for segment A.
- Hardware ID 4 will be assigned for segments B and C.

Note: Only individual segments can be assigned to a card format, not segment groups.

The rules for card format segmentation are:

- A user can only place a card format into segments to which they have access. Only an <All Segments> user can place a format into <All Segments>.
- A user must have access to all segments to which a card format belongs in order to modify or delete it. Only an <All Segments> user may modify or delete a card format assigned to <All Segments>.
- A user can view any card format that belongs to at least one segment to which the user has access. Any user can view an <All Segments> card format.
- A user can assign any card format that they can view to a badge type and a reader.

Badge Type Segmentation

If badge types are segmented, badges are also segmented by virtue of their type. If not segmented, badges and badge types are considered system-wide and available to all cardholders and users. A badge type is assigned a primary segment that can be <All Segments>, an individual segment, or a segment group. It can also be assigned additional segments and segment groups.

The rules of badge type segmentation are:

- A user can only place a badge type into segments for which they have access. Only an <All Segments> user can place a badge type into <All Segments>.
- A user must have access to all segments in which a badge type belongs in order to modify or delete it. Only an <All Segments> user may modify or delete a badge type assigned to <All Segments>.
- A user can view any badge type that belongs to at least one segment to which the user has access. Any user can view an <All Segments> badge type.
- A user must have access to the primary segment of the badge type in order to assign it to a badge, modify a badge, or delete a badge with that type. Only an <All Segments> user can assign an <All Segments> badge type, or modify or delete a badge having an <All Segments> badge type.
- A user can view any badge having a badge type that belongs to at least one segment to which the user has access. Any user can view a badge having an <All Segments> badge type format.
- A user can modify access level assignments to any badge that they can view.

- A badge can only be assigned access levels that belong in segments to which its badge type also belongs.

Notes: If a user attempts to remove a badge type from a segment, all existing badges having that type are no longer eligible to have access levels in that segment.

If you are using a segmented system, for the badge type to appear as a selection in Visitor Administration, its primary segment should be **All Segments**.

Cardholder Segmentation

When cardholders are segmented, they are assigned a primary segment that can be <All Segments>, an individual segment, or a segment group. A cardholder can also be assigned additional segments and segment groups. Since a cardholder's primary segment assignment dictates the segment access necessary to edit the cardholder, it should fully represent the true organizational membership of the cardholder in terms of segments. Additional segment assignments outside of the primary segment are useful for accommodating common landlord segment access in a tenant/landlord scenario, and other specialized cardholder access needs.

The rules of cardholder segmentation are:

- A user can view any cardholder that belongs to at least one segment to which the user has access. Any user can view an <All Segments> cardholder.
- A user can only place a cardholder into segments to which they have access. Only an <All Segments> user can place a cardholder into <All Segments>.
- A user must have access to a cardholder's primary segment in order to do any of the following operations:
  - Modify or delete a cardholder.
  - Add, modify, or delete badges for the cardholder.
  - Assign assets, modify and delete asset assignments.
  - Capture multimedia and biometrics.
  - Link directory accounts to the cardholder.
  - Print or encode badges.

Note: Only an <All Segments> user may perform these operations for a cardholder assigned to <All Segments>.

- A user who can view a cardholder can perform the following operations on any cardholder they can view; however, they can only affect assignments for segments to which the user has access:
  - Modify access and precision access levels.
  - Modify guard tour group assignments.
  - Issue “one free pass” for anti-passback.
  - Do an anti-passback move badge.
  - Display global anti-passback areas.
- Any badge owned by the cardholder can only be assigned access levels that belong in segments to which the cardholder also belongs.
- If badge types are also segmented, a cardholder can only be assigned a badge type with which it has at least one segment in common. Only an <All Segments> cardholder can be assigned an <All Segments> badge type.

When a user attempts to remove a cardholder from one or more segments:

- If the cardholder is no longer eligible to own one of the badges they currently own (due to badge type segmentation), the change is not allowed. The user must either delete the badge that is in violation or adjust the cardholder or badge type segment assignments.
- Any access levels from the removed segments must be unassigned from all badges owned by the cardholder.

Visitor Segmentation

If cardholders are segmented, visitors can optionally be segmented as well. If they are not segmented, they are considered system-wide and available to all cardholders and users. In a single organization, it may make sense not to segment visitors to reduce the chances of the same visitor being entered multiple times in the system. For a tenant/landlord system, it would make sense to segment visitors.

When visitors are segmented, they follow the same rules as for cardholders in regards to which users can edit them, which badge types can be assigned, and what access levels can be assigned. In addition:

- If a user can view a cardholder and a visitor, they are allowed to assign a visit between them. A user does not need access to the primary segment of either cardholder or visitor to setup a visit between them.
- A cardholder and a visitor must have at least one segment in common in order to establish a visit between them. If an existing visitor is visiting a new cardholder that has different segment assignments, one common segment must be established between them.
- A user must have segment access to view both the cardholder and the visitor in order to view individual visit records.
- When a user is adding a visitor in the context of adding a visit to a cardholder, the visitor’s default segment assignments will be set to those of the cardholder being visited for which the user also has access. The user will be able to edit the segment assignments with proper permissions. If the user does not have access to the cardholder's primary segment, they must assign a different primary segment to the visitor so that they can edit the visitor later.
- The same access level availability rules must be enforced for segmented visitors; they can only have access levels in the segments assigned to them. Therefore, if reusable access control badges are being used, the currently assigned access levels for those badges may need to be adjusted upon assignment to a visitor.

When cardholders are segmented but visitors are not:

- All users can view and edit any visitor.
- Even though the user can view a visitor, a user can only see visits to cardholders that they are allowed to view.
- Any cardholder can have any visitor visit them.
- A visitor can have any badge type and access levels assigned to them.
- If a user can view a cardholder, they can assign a visit to them. A user does not need access to the primary segment of the cardholder to be able to setup a visit for them.

Allowing Access Levels to Be Assigned by Users in Other Segments

This feature gives a landlord a flexible per access level and per segment granularity of control. A typical tenant/landlord scenario includes common readers for areas that every tenant must have access to, such as front doors for entrance into a building. One way to approach this is:

- The landlord creates one or more “landlord segments” in which common devices are placed. Access levels for these segments are also created, such as “Building 1 Lobby Doors”.

- A landlord segment group is created to contain the one or more landlord segments.
- The landlord segment group is assigned as an additional segment assignment to all applicable tenant badge types (if segmented) and tenant cardholders. This allows access levels from the common landlord segments to be assigned to tenant badges.

In some scenarios, only landlord personnel are allowed to assign and remove access levels from tenant badges. However, what if the landlord wishes to allow tenants to control their cardholder's access to common areas? The landlord cannot give tenant users access to landlord segments. Since all cardholders will be assigned landlord segments in order to gain access, this would allow tenants to see each others' cardholders.

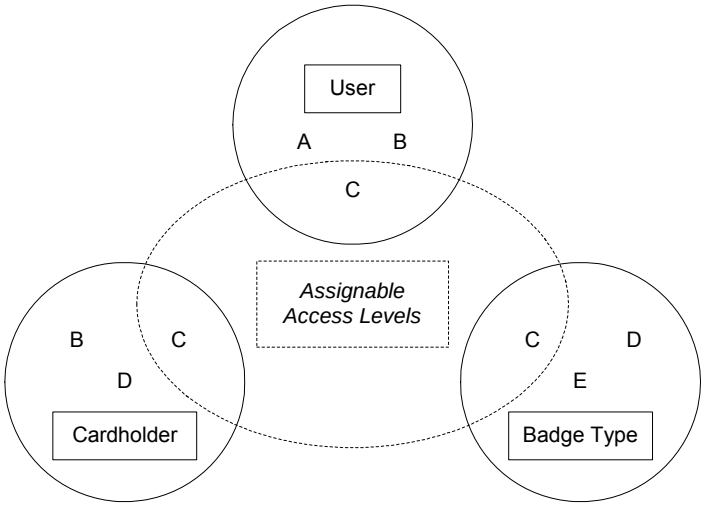
To accommodate this need, landlords have the option of allowing access levels to be configured as assignable by users in other segments. The landlord can use this option to make individual access levels from landlord segments assignable by tenant users. For example, the landlord can make “Building 1 Lobby Doors” assignable by any tenants in building 1 by selecting those tenant segments as being allowed to assign that level.

Note: The cardholder still must have access to the segment in order for a level to be assigned. Currently, this requires landlord involvement when a new cardholder record is first added. The landlord must grant the cardholder access to the appropriate landlord segments.

Assigning Access Levels Example

One of the key features of cardholder segmentation is controlling which access levels can be assigned to a badge based on the segment membership of users, badge types (if also segmented), and cardholders. For example, assuming that both badge types and cardholders are segmented and:

- The user belongs to segment group ABC only.
- The cardholder's primary segment is group BCD with no additional assignments.
- The badge type's primary segment is group CDE with no additional assignments.



The user can only assign and remove access levels in segment C, since it is the only common segment between the user, the cardholder, and the badge type.

Note: In this scenario, the user cannot do anything to this cardholder but assign/remove access levels since the user does not have full access to the cardholder's primary segment assignment.

Choosing Segmentation - Ramifications and Process Flow

Segmentation is an option that is system-wide for a single database. Ideally, new installations that intend to use segmentation will configure their systems for segmentation prior to going online in a “live” (i.e., real data) environment.

• *WARNING!* • Existing installations can convert to segmentation mode. However, once segmentation has been enabled, it PERMANENTLY changes the database, and CANNOT be disabled. YOUR ORGANIZATION SHOULD BE CERTAIN THAT YOU WISH TO USE SEGMENTATION BEFORE YOU INITIATE THE CONVERSION.

Process Outline - New Installations

If you are a new customer, it’s best to create your segmented system methodically, as follows:

1. Decide whether segmentation is appropriate for your environment. If it is, it is strongly recommended that you first read through this entire chapter to fully comprehend the impact of segmentation.
2. Enable segmentation.
3. Define segments.
4. Configure your system, adding users, cardholders, and hardware and other objects. Refer to the previous, numbered chapters in this user guide for assistance. As you add objects, you will be prompted to choose a segment if the object is affected by segmentation.

Note: For more information, refer to Chapter 18: Segments Folder on page 453.

Process Outline - Existing Installation

If you already have a non-segmented system in place, you can convert it to a segmented system in the following manner:

1. Decide whether segmentation is appropriate for your environment. If it is, it is strongly recommended that you first read through this entire chapter to fully comprehend the impact of segmentation. Then:
2. Enable segmentation.
3. Define segments.
4. Move access panels and copy objects to the new segments. When adding a segment, you have the opportunity to move access panels and copy related objects from the current database and assign them to the new segment. It is assumed that the access panels and objects you select for this process are all currently in the same segment.

   IMPORTANT: If you move access panels from one segment (for example, Segment A) but copy objects from a different segment (such as Segment B), all links between the selected access panels and their related objects will be LOST. This is something that you will probably never want to do.

5. Assign each user to a specific segment.

Note: For more information, refer to Chapter 18: Segments Folder on page 453.

Object Segmentation Table

The following table lists all OnGuard objects and their segmentation characteristics. There are several types of segmentation, including:

- **Single** - Contain one segment assignment and cannot be a segment group. Depending on the object, <All Segments> may be allowed.
- **Implicit** - Segmented based on its parent object (sharing the same characteristics of parent object.)
- **Single assignment, multiple via segment groups**. Users can choose only one segment assignment. However, the segment assignment can be a segment group (indirectly allowing multiple segment assignments).
- **Multiple assignments, which may or may not be segment groups**. Most objects that allow multiple assignments allow both segments and segment groups to be assigned, with the exception of card formats which only allow segments to be assigned.

Object	Can be Segmented?	Type of Segmentation	<All Segments> Allowed?	Comments	Segmented Objects Assigned/ Linked
Access Groups	Yes	Single	Yes		Access Levels
Access Levels	Yes	Single	No		Readers, Timezones
Access Panels	Yes	Single	No		Timezones (dialup)
Action Groups	Yes	Single assignment, multiple via Segment Group	Yes		Actions
Actions	Yes	Single assignment, multiple via Segment Group	Yes	Segment restrictions may depend on the type of action.	Dependent on the type of action
Alarm Acknowledgments	Yes	Implicit	NA		NA
Alarm Inputs	Yes	Implicit	NA		Timezones, Outputs
Alarm Mask Groups	Yes	Implicit	NA		NA
Alarm Outputs	Yes	Implicit	NA		NA
Alarm Panels	Yes	Implicit	NA		NA
Alarm Priority Range/Colors	No	NA	NA		NA

Object	Can be Segmented?	Type of Segmentation	<All Segments> Allowed?	Comments	Segmented Objects Assigned/ Linked
Alarms	Yes	Single	Yes		Devices, Function Lists (for acknowledgment actions)
Archive Configurations	No	NA	NA		NA
Archive History	No	NA	NA		NA
Areas (APB)	Yes	Implicit	NA		NA
Asset Classes	No	NA	NA		NA
Asset Groups	No	NA	NA		NA
Asset Subtypes	No	NA	NA		NA
Asset Types	No	NA	NA		NA
Assets	No	NA	NA		NA
Audio for Alarms	No	NA	NA		NA
Authorization Options for Login	No	NA	NA		NA
Badge Access Level Assignments	Yes	Implicit	NA		NA
Badge Layout Graphics	No	NA	NA		NA
Badge Layouts	No	NA	NA		NA
Badge Precision Access Level Assignments	Yes	Implicit	NA		NA
Badge Status List	No	NA	NA		NA
Badge Types	Yes	Optional, multiple and segment groups	Yes		Access Group, Card Formats
Badges	Yes	Implicit via badge type	NA		Access Levels, Precision Access Groups
Card Formats	Yes	Optional, multiple, but no segment groups.	Yes		NA
Cardholder Last Location	No	NA	NA		NA

Object	Can be Segmented?	Type of Segmentation	<All Segments> Allowed?	Comments	Segmented Objects Assigned/ Linked
Cardholder Multimedia Objects	Yes	Implicit	NA		NA
Cardholder	Yes	Optional, multiple and segment groups	Yes		Badges
CCTV	No	NA	NA		NA
Device Group	Yes	Single	Yes		Devices, based on panel type
Digital Video Archive Server	Yes	Single	No		NA
Downloadable Reader Formats	Yes	Single	No		NA
Elevator Control Levels	Yes	Single	No		Timezones
EOL Resistor Tables	Yes	Single	No		NA
Encoders	No	NA	NA		NA
Event History	Yes	Implicit	NA		NA
Event Routing Groups	Yes	Single	Yes		Timezones
Event Types	No	NA	NA		NA
Event Definitions	No	NA	NA		NA
Failed Panel Downloads	No	NA	NA		NA
Fire Devices	Yes	Implicit	No	Based on panel	NA
Fire Panels	Yes	Single	No		NA
Global I/O Function Lists	Yes	Implicit	NA		NA
Global I/O Programming	Yes	Implicit	NA		NA
Global Linkages	Yes	Single assignment, multiple via Segment Group	Yes	Affects which segmented items can be linked.	Any device, action, etc., supported.
GOS Alarm Messages	No	NA	NA		NA

Object	Can be Segmented?	Type of Segmentation	<All Segments> Allowed?	Comments	Segmented Objects Assigned/ Linked
GOS Device	No	NA	NA		NA
GOS Messages	No	NA	NA		NA
GOS Recipient Address	No	NA	NA		NA
GOS Recipients	No	NA	NA		NA
Holidays	Yes	Single	No		NA
Holiday Types	No	NA	NA		NA
Intercom Exchanges	Yes	Implicit	NA		NA
Intercom Stations	Yes	Single	No		NA
Intrusion Areas	Yes	Implicit	No	based on intrusion panel	NA
Intrusion Doors	Yes	Implicit	No	based on intrusion panel	NA
Intrusion Offboard Relays	Yes	Implicit	No	based on intrusion panel	NA
Intrusion Onboard Relays	Yes	Implicit	No	based on intrusion panel	NA
Intrusion Panels	Yes	Single	No		Intrusion Panel User Groups
Intrusion Panel User Groups	Yes	Single	Yes		NA
Intrusion Zone	Yes	Implicit	Yes	Based on intrusion panel	NA
Local I/O Function Lists	Yes	Implicit	No	Based on parent panel	NA
Local I/O Programming	Yes	Implicit	No	Based on parent panel	NA
Map Icons	No	NA	NA		NA
Maps	Yes	Single assignment, multiple via segment group	Yes		Devices (based on parent panel), other maps
Monitor Station Saved Events	No	NA	NA		NA
Monitor Stations	No	NA	NA		NA

Object	Can be Segmented?	Type of Segmentation	<All Segments> Allowed?	Comments	Segmented Objects Assigned/ Linked
Monitor Zones	Yes	Single assignment, multiple via segment group	Yes		Devices, Event Routing Group
Multimedia Object Types	No	NA	NA		NA
OPC Connections	Yes	Single	No		NA
OPC Sources	Yes	Implicit	No	Based on OPC Connection	NA
DataConduIT Sources	Yes	Single	No		NA
Personal Safety Panels	Yes	Single	No		NA
Personal Safety Transmitters	No	NA	NA		NA
Precision Access Groups	Yes	Single	No		Readers, Timezones
Reader/Timezone Modes	Yes	NA	No		NA
Readers	Yes	NA	No		Card Formats, Timezones, Elevator Levels, Downloadable Reader Formats
Receiver Accounts	Yes	Single	No		Event Code Templates and Receiver Account Groups
Receiver Account Groups	Yes	Single	No		Receiver Accounts
Receiver Event Code Templates	Yes	Single assignment, multiple via Segment Group	Yes		NA
Receivers	Yes	Single	No		NA
Receivers Areas	Yes	Implicit	NA	Based on receiver account	NA

Object	Can be Segmented?	Type of Segmentation	<All Segments> Allowed?	Comments	Segmented Objects Assigned/ Linked
Receiver Zones	Yes	Implicit	NA	Based on receiver account	NA
Reports	No	NA	NA		NA
Restored Alarm Acknowledgments	Yes	Implicit	NA		NA
Restored Event History	Yes	Implicit	NA		NA
Restored User Transactions	Yes	Implicit	NA		NA
Segments	Yes	Single	Yes		NA
SNMP Agents	Yes	Single	No		NA
SNMP Management Base	Yes	Single	Yes		NA
SNMP Managers	Yes	Single	No		NA
System Cardholder Configuration	No	NA	NA		NA
System Configuration	Yes	Some system configuration is per-segment when segmentation is enabled	NA		NA
Text Objects for Alarm Monitoring	No	NA	NA		NA
Tour Groups	Yes	Single	No		NA
Tours	Yes	Single	No		NA
Timezones	Yes	Single	No		NA
UDF drop-down lists	No	NA	NA		NA
UDF Layouts (includes database table/field definitions, pages, and UI layouts for cardholders, visitors, and assets	No	NA	NA		NA
User Permission Groups	Yes	Single	Yes		NA

Object	Can be Segmented?	Type of Segmentation	<All Segments> Allowed?	Comments	Segmented Objects Assigned/ Linked
User Transactions	Yes	Implicit based on user in transaction	NA		Permission Groups, Area Access Manager Levels
Users	Yes	Multiple and segment groups	Yes		NA
Video Cameras	Yes	Implicit	NA		Device/ Camera Links, Matrix Switchers
Video Matrix Switchers	Yes	Single	No		NA
Video Monitors	Yes	Implicit	No		NA
Video Servers	Yes	Single	No		NA
Visitors	Yes	Optional, multiple and segment groups	Yes		Cardholders (for visitor visits)
Workstations	No	NA	NA		NA

APPENDIX F

ASCII Character Chart

ASCII Values 0-127

Refer to the following table for ASCII values 0-127. For more ASCI values, refer to ASCII Values 128-255 on page 1434.

ASCII Values 0-127

ASCII Value	Control Character	Control Action
0	NUL	Null character
1	SOH	Start of heading, = console interrupt
2	STX	Start of text, maintenance mode on HP console
3	ETX	End of text
4	EOT	End of transmission, not the same as ETB
5	ENQ	Enquiry, goes with ACK; old HP flow control
6	ACK	Acknowledge, clears ENQ logon hang
7	BEL	Bell, rings the bell
8	BS	Backspace, works on HP terminals/computers
9	HT	Horizontal tab, move to next tab stop
10	LF	Line Feed
11	VT	Vertical tab
12	FF	Form Feed, page eject
13	CR	Carriage Return
14	SO	Shift Out, alternate character set
15	SI	Shift In, resume default character set

ASCII Values 0-127 (Continued)

ASCII Value	Control Character	Control Action
16	DLE	Data link escape
17	DC1	XON, with XOFF to pause listings; "okay to send"
18	DC2	Device control 2, block-mode flow control
19	DC3	XOFF, with XON is TERM=18 flow control
20	DC4	Device control 4
21	NAK	Negative acknowledge
22	SYN	Synchronous idle
23	ETB	End transmission block, not the same as EOT
24	CAN	Cancel line, MPE echoes!!!
25	EM	End of medium, Control-Y interrupt
26	SUB	Substitute
27	ESC	Escape, next character is not echoed
28	FS	File separator
29	GS	Group separator
30	RS	Record separator, block-mode terminator
31	US	Unit separator
32	SP	Space
33	!	Exclamation mark
34	"	Quotation mark (" in HTML)
35	#	Cross hatch (number sign)
36	$	Dollar sign
37	%	Percent sign
38	&	Ampersand
39	‘	Closing single quote (apostrophe)
40	(	Opening parentheses
41	)	Closing parentheses
42	*	Asterisk (star, multiply)
43	+	Plus
44	,	Comma
45	-	Hyphen, dash, minus

ASCII Values 0-127 (Continued)

ASCII Value	Control Character	Control Action
46	.	Period
47	/	Slant (forward slash, divide)
48	0	Zero
49	1	One
50	2	Two
51	3	Three
52	4	Four
53	5	Five
54	6	Six
55	7	Seven
56	8	Eight
57	9	Nine
58	:	Colon
59	;	Semicolon
60	<	Less than sign (< in HTML)
61	=	Equals sign
62	>	Greater than sign (> in HTML)
63	?	Question mark
64	@	At-sign
65	A	Uppercase A
66	B	Uppercase B
67	C	Uppercase C
68	D	Uppercase D
69	E	Uppercase E
70	F	Uppercase F
71	G	Uppercase G
72	H	Uppercase H
73	I	Uppercase I
74	J	Uppercase J
75	K	Uppercase K

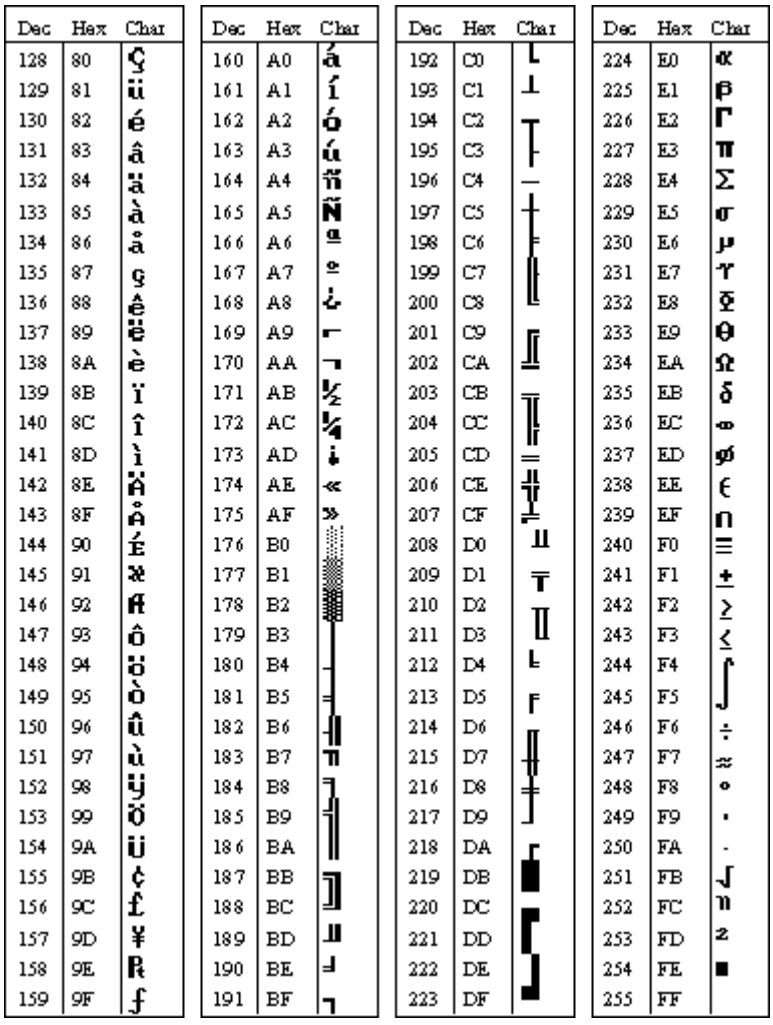
ASCII Values 0-127 (Continued)

ASCII Value	Control Character	Control Action
76	L	Uppercase L
77	M	Uppercase M
78	N	Uppercase N
79	O	Uppercase O
80	P	Uppercase P
81	Q	Uppercase Q
82	R	Uppercase R
83	S	Uppercase S
84	T	Uppercase T
85	U	Uppercase U
86	V	Uppercase V
87	W	Uppercase W
88	X	Uppercase X
89	Y	Uppercase Y
90	Z	Uppercase Z
91	[	Opening square bracket
92	\	Reverse slant (Back slash)
93	]	Closing square bracket
94	^	Caret (Circumflex)
95	_	Underscore
96	‘	Opening single quote
97	a	Lowercase a
98	b	Lowercase b
99	c	Lowercase c
100	d	Lowercase d
101	e	Lowercase e
102	f	Lowercase f
103	g	Lowercase g
104	h	Lowercase h
105	i	Lowercase i
106	j	Lowercase j

ASCII Values 0-127 (Continued)

ASCII Value	Control Character	Control Action
107	k	Lowercase k
108	l	Lowercase l
109	m	Lowercase m
110	n	Lowercase n
111	o	Lowercase o
112	p	Lowercase p
113	q	Lowercase q
114	r	Lowercase r
115	s	Lowercase s
116	t	Lowercase t
117	u	Lowercase u
118	v	Lowercase v
119	w	Lowercase w
120	x	Lowercase x
121	y	Lowercase y
122	z	Lowercase z
123	{	Opening curly brace
124	|	Vertical line
125	}	Closing curly brace
126	~	Tilde (approximate)
127	DEL	Delete (rub out), cross-hatch box

ASCII Values 128-255



Dec	Hex	Char
128	80	Ç
129	81	ü
130	82	é
131	83	â
132	84	ä
133	85	à
134	86	å
135	87	ç
136	88	ê
137	89	ë
138	8A	è
139	8B	ï
140	8C	î
141	8D	ì
142	8E	Ä
143	8F	Å
144	90	É
145	91	æ
146	92	Æ
147	93	ô
148	94	ö
149	95	ò
150	96	û
151	97	ù
152	98	ÿ
153	99	Ö
154	9A	Ü
155	9B	¢
156	9C	£
157	9D	¥
158	9E	₧
159	9F	ƒ

Dec	Hex	Char
160	A0	á
161	A1	í
162	A2	ó
163	A3	ú
164	A4	ñ
165	A5	Ñ
166	A6	ª
167	A7	º
168	A8	¿
169	A9	⌐
170	AA	¬
171	AB	½
172	AC	¼
173	AD	¡
174	AE	«
175	AF	»
176	B0	▒
177	B1	▒
178	B2	▒
179	B3	│
180	B4	┤
181	B5	╡
182	B6	╢
183	B7	╖
184	B8	╕
185	B9	╣
186	BA	║
187	BB	╗
188	BC	╝
189	BD	╜
190	BE	╛
191	BF	┐

Dec	Hex	Char
192	C0	└
193	C1	┴
194	C2	┬
195	C3	├
196	C4	─
197	C5	┼
198	C6	╞
199	C7	╟
200	C8	╚
201	C9	╔
202	CA	╩
203	CB	╦
204	CC	╠
205	CD	═
206	CE	╬
207	CF	╧
208	D0	╨
209	D1	╤
210	D2	╥
211	D3	╙
212	D4	╘
213	D5	╒
214	D6	╓
215	D7	╫
216	D8	╪
217	D9	┘
218	DA	┌
219	DB	▒
220	DC	▒
221	DD	▒
222	DE	▒
223	DF	▒

Dec	Hex	Char
224	E0	α
225	E1	ß
226	E2	Γ
227	E3	π
228	E4	Σ
229	E5	σ
230	E6	µ
231	E7	τ
232	E8	Φ
233	E9	Θ
234	EA	Ω
235	EB	δ
236	EC	∞
237	ED	ø
238	EE	ε
239	EF	∩
240	F0	≡
241	F1	±
242	F2	≥
243	F3	≤
244	F4	⌠
245	F5	⌡
246	F6	÷
247	F7	≈
248	F8	°
249	F9	∙
250	FA	·
251	FB	√
252	FC	ⁿ
253	FD	²
254	FE	■
255	FF	

APPENDIX G

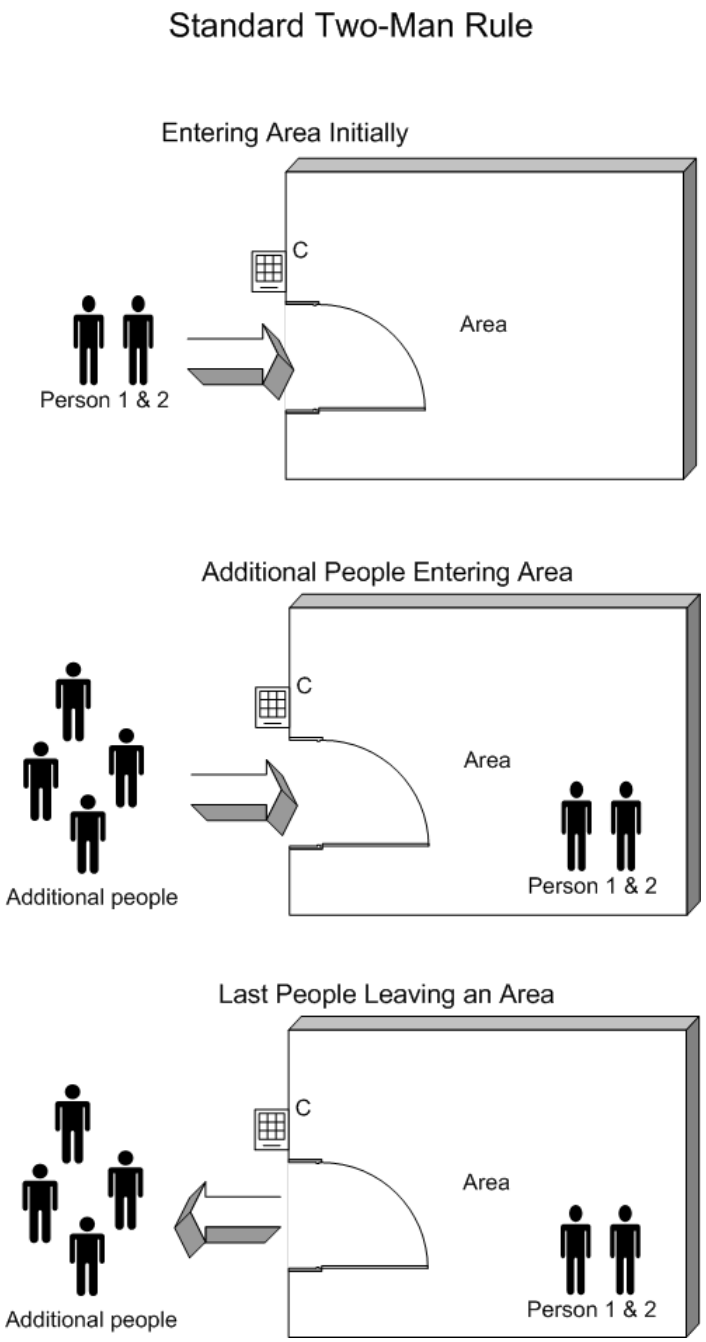
Special Two-Man Rule

The Special Two-Man Rule is an extension of the existing Two-Man Rule that exists for local anti-passback (APB). The special functionality is designed to control who has access to special areas when in the special two-man control modes.

Standard Two-Man Rule Overview

In Standard Two-Man Rule, when an area is empty two people are required to enter the area at the same time and after additional people can enter the area. When leaving, the last two people must leave the room at the same time. This is so there are always at least two people in the room at the same time.

The following diagram illustrates how Standard Two-Man Rule works:



Special Two-Man Rule Overview

Special Two-Man Rule adds two additional special modes to how Standard Two-Man Rule works: Special 1-Man Mode and Special 2-Man Mode. These special modes use different classifications of individuals: Team Members, Supervisors, and Others.

Definitions

- *Area Owner* - The area owner is a team member who, once in the area, allows the other team members to enter without approval from inside.
- *Team Member* - Team members are the cardholders allowed into the areas that are configured for the special 1-man or 2-man rules.
- *Supervisors* - Supervisors are individuals who are allowed inside of areas that are configured for the special 1-man or 2-man rules but need approval from someone inside of the area.
- *Others* - Others are individuals who are not allowed inside of areas that are configured for the special 1-man or 2-man rules.

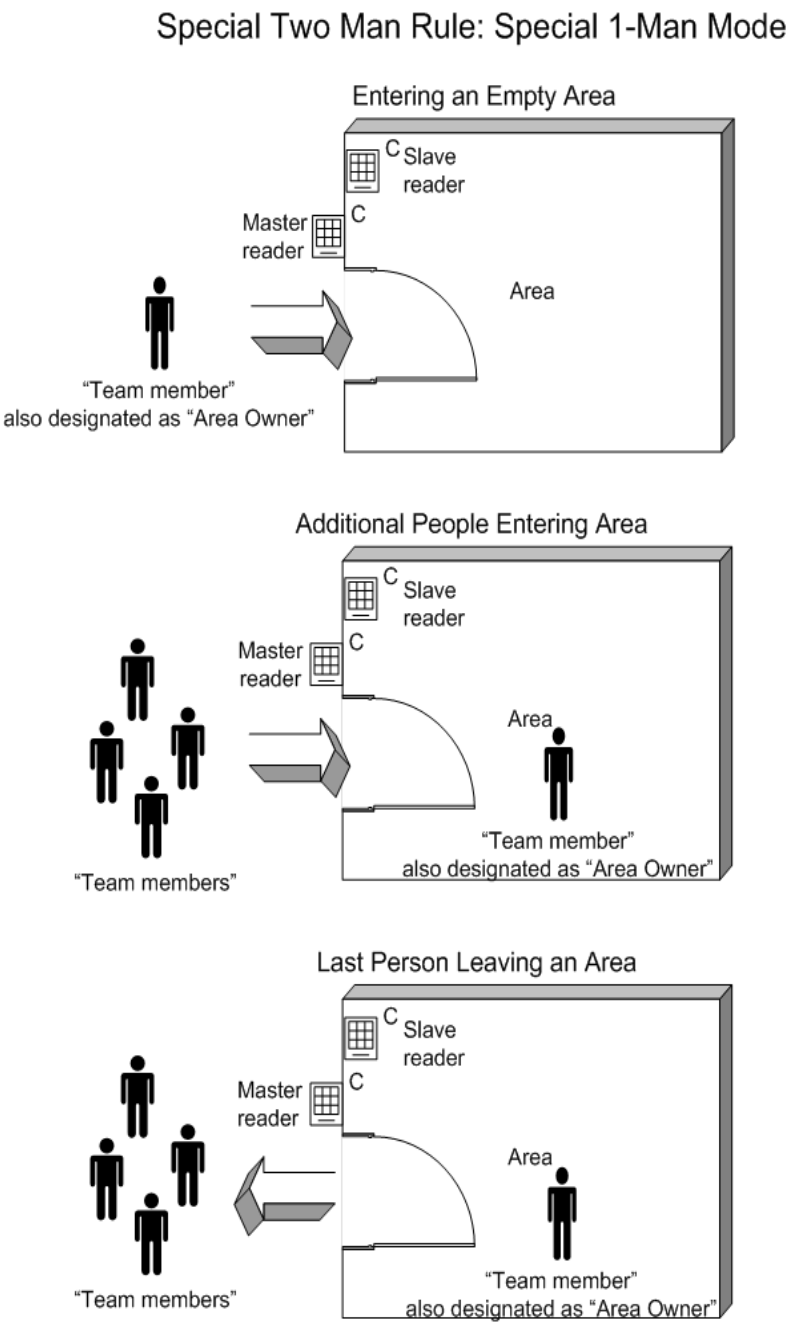
Special 1-Man Mode

In the Special 1-Man Mode, a special “Team Member” is configured to be the “Area” or “Assigned” owner to a specific area. This “Area Owner” must be the first individual to enter the area and the last individual to exit the area. Once the assigned Area Owner is inside the area, other Team Members or Supervisors are allowed to enter the area.

When the assigned Area Owner is in the area and a Supervisor attempts access, a strobe inside the area fires and enables the door release push-button within the room.

Individuals who are classified as Others are not allowed access to the area when in this mode.

The following diagram illustrates how Standard Two-Man Rule: 1-Man Mode works:



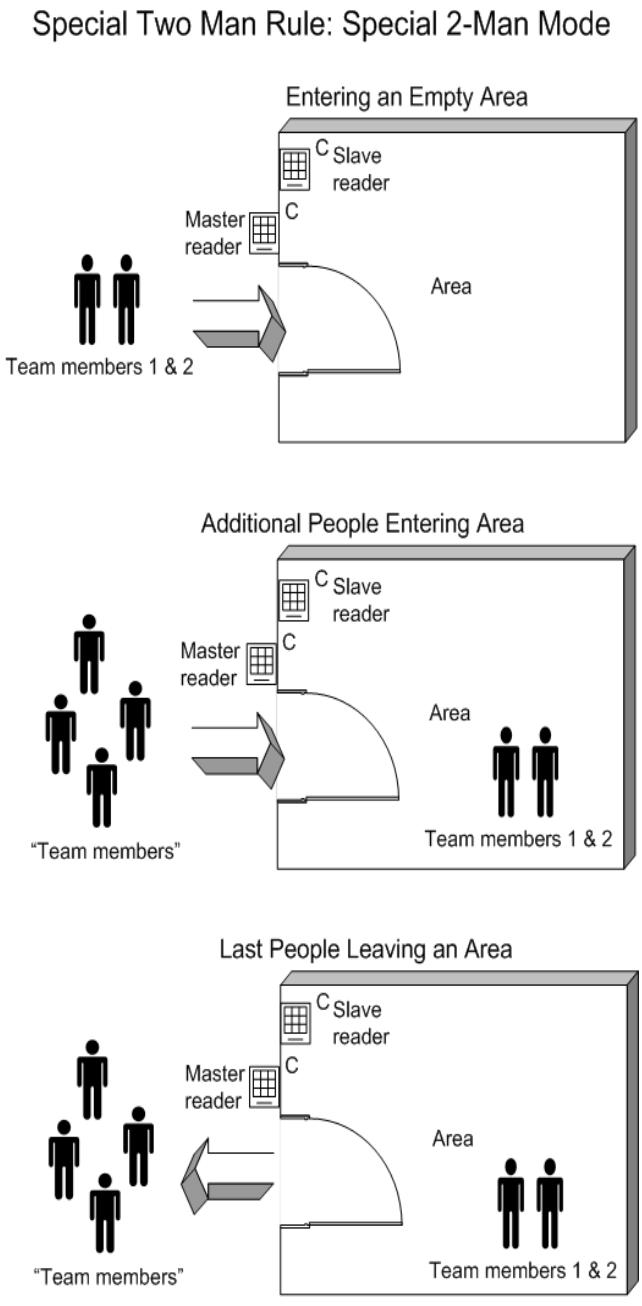
Special 2-Man Mode

In the Special 2-Man Mode, the first two individuals into the area must be Team Members and the last two individuals to leave the area must also be Team Members. Once two Team Members are inside the area, additional Team Members or Supervisors are allowed access.

When a Supervisor attempts access and there are at least two Team Members in the area, a strobe inside the area fires and enables the door release push-button within the room.

Individuals who are classified as Others are not allowed access to the area when in this mode. The last two individuals who leave the area must be Team Members.

The following diagram illustrates how Standard Two-Man Rule: 2-Man Mode works:



Note: The first two Team members that enter do not have to be the same two Team members that leave.

Special Two-Man Rule Configuration Instructions

Before configuring Special Two-Man Rule in the OnGuard software, you must configure the readers for Special Two-Man Rule.

- The Master reader is the reader being used to enter the area.
- The Slave reader is the reader being used to exit the area.

For more information, refer to the Hardware Configuration Guide.

To complete the software configuration, do the following steps or consult the quick-configuration table below:

Configuration step	Software location
1. Configure the Access Panels for Special Two-Man Rule on page 1440.	Access Control > Access Panels > Access panel type > Options form
2. Configure the Areas for Special Two-Man Rule on page 1440 for Special 1-Man Mode or Special 2-Man Mode.	Access Control > Areas > Anti-Passback Areas form
3. Configure the Readers for Special Two-Man Rule on page 1441 to configure the readers as master and slave.	Access Control > Readers > Settings form
4. Optional: Configure the List Builder for Special Two-Man Rule on page 1441. By default, there are two badge types: “Supervisor” and “Team Member”. You may configure additional badge types if necessary.	Administration > List Builder
5. (Optional) Configure the Timezone for Special Two-Man Rule on page 1442.	Access Control > Timezones > Timezone/Area Modes form

Configure the Access Panels for Special Two-Man Rule

In the System Administration menu bar select ***Access Control*** > ***Access Panels***. Choose your access panel and go to its Options form. A **Special area rules** check box is present on the form. Select it to enable the Two-Man Rule on the access panel.

Note: This feature is only available for Lenel access panels

After the **Special area rules** check box has been checked for the first time, you will receive the following message:

Configure the Areas for Special Two-Man Rule

In the System Administration menu bar select, ***Access Control*** > ***Areas***. On the Anti-Passback Areas sub-tab, the **Two man control** drop-down box allows you to configure areas so they adhere to the Special 1-Man or Special 2-Man rules.

For more information, refer to Areas Form (General Sub-tab) on page 756.

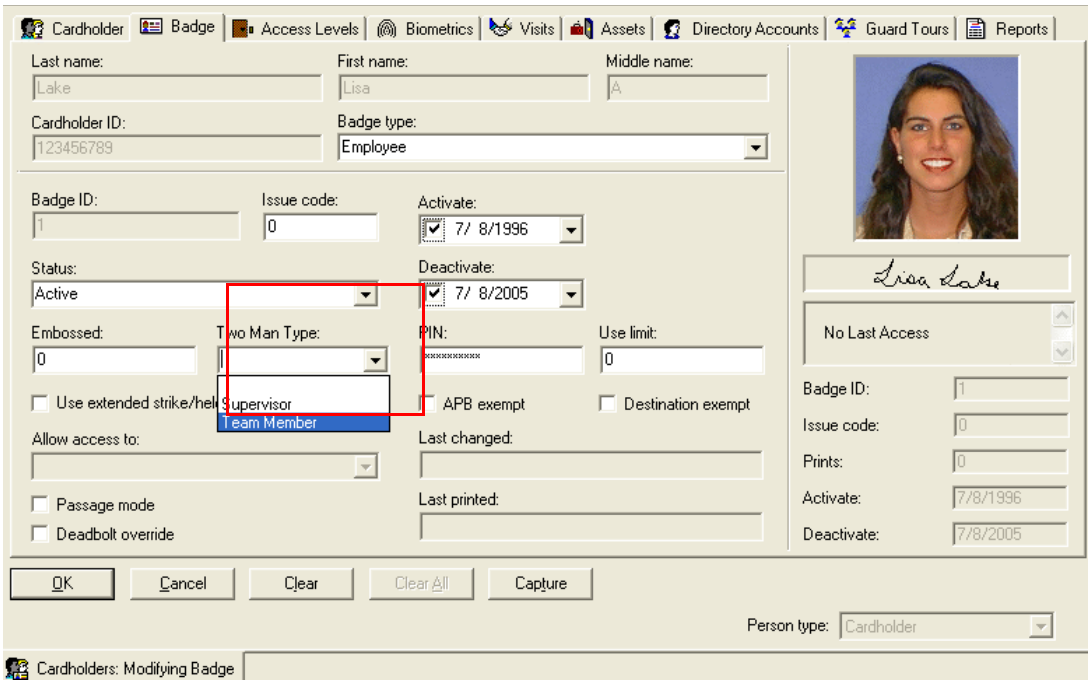
With the access panels configured a new sub-tab appears in the Areas folder. This Special Two Man sub-tab allows you to configure the timeout used for the strobe by changing the **Occupant approval timeout** spin button, which can be configured between 1 and 255 seconds.

The area owner can also be configured in the Assigned owner section when the area is in 1-man mode. The area owner is a team member who, once in the area, allows the other team members to enter without approval from inside.

For more information, refer to Special Two Man Form on page 775.

Configure the Badges for Special Two-Man Rule

In the System Administration menu bar select ***Administration*** > ***Cardholders***. On the Badge tab, assign the appropriate **Two Man Type** designation for specific cardholders



Configure the Readers for Special Two-Man Rule

To configure the readers you must configure them to be master and slave. The entering reader must be configured as a “paired master” and the exit reader must be a “paired slave”

In the System Administration menu select ***Access Control*** > ***Readers***. In the Settings tab, select the reader and select the appropriate (Paired Master and Paired Slave) check box in the settings section of the form.

For more information, refer to Settings Form on page 645.

Configure the List Builder for Special Two-Man Rule

This step is optional and does not have to be done.

To configure lists for the Two Man Type badge types select ***Administration*** > ***List Builder***. You cannot delete or modify the default list items but you can add list items, which will be treated as “Others” who are usually not allowed in special areas.

For more information, refer to List Builder Folder on page 481.

Configure the Timezone for Special Two-Man Rule

This step is optional and does not have to be done.

To change the Special Two-Man Rule based on date and time you must use the Timezone/Area Modes sub-tab. This is found by selecting ***Access Control > Timezones*** in the System Administration menu bar.

By modifying the Timezone/Area you can select what area is going to be changed according to a Timezone you specify.

For more information, refer to Timezone/Area Modes Form on page 715.

APPENDIX H

Inline Encoding

Windows is capable of handling standard print information sent by OnGuard to the printer. When added information is needed for special functions such as magnetic and smart card encoding, special commands are required. Mapping of the printer driver name to the printer type name is necessary for OnGuard to send the appropriate commands for that printer. This appendix contains advanced information for system administrators. General users of OnGuard will not need to reference this section.

Note: Fargo printers require mapping to the printer type name for all badge printing.

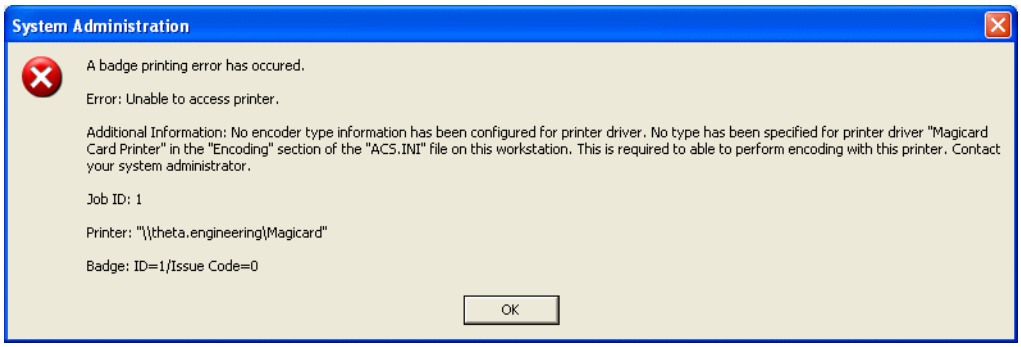
To configure the system for printing with smart card encoders, refer to the section Direct Printers with Inline Encoders on page 1450.

Modify the Encoding section of ACS.INI

IMPORTANT: Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

When encoding via a card printer, there must be an entry in the Encoding section of the **ACS.INI** file for the printer driver of the card printer. This entry specifies the driver name and the OnGuard printer type. The Encoding section is populated with common print driver versions however, when new driver versions are released, it may be necessary to add new entries.

1. A badge printing error will be displayed when encoded information is sent to a print driver not listed in the **ACS.INI** file:



2. Note printer driver name in quotes. This name is specific to the printer you are using and will be part of the line that needs to be added to the **ACS.INI** file.
3. Click the Start menu, select ***Run***.
4. In the Run dialog, type `ACS.INI`. Click [OK].
5. Find the section labeled `[Encoding]` and add the line:

   `<printer driver>=<printer type name>`

   where *<printer driver>* equals the name from the error message above and *<printer type name>* equals the Printer type name from the following table (for example, Magicard Card Printer=MagicCard).

Printer Type Name	Applicable Card Printer Models
DataCard	Discontinued DataCard models where the driver name is not “SmartDriver”
Evolis	All Evolis printers
Digid	All Magicard Prima models except Prima 4
GenericISO7811	Kodak/JVC/Fargo/Eltron GenericISO7811 should only be used for legacy Eltron models using a driver named “PRIV300” or “PRIV400”
ImageCardExpress	All DataCard models using a driver named “SmartDriver”
MagicCard	All Magicard models except Prima
Nisca	All NiSCA models
Persona	All Fargo models
PrivilegeNT	All Zebra (formerly called Eltron) models except for drivers named “PRIV300” or “PRIV400”

Standard Magnetic Format Attributes

The following set of attributes are used for magnetic track encoding:

1. Magnetic format: bits/inch, bits/character, character parity, use of an LRC and LRC parity.
   a. The standard magnetic format for IATA is 210 bits/inch, 7 bits/character, odd character parity and LRC with even parity.

b. The standard magnetic format for ABA is 75 bits/inch, 5 bits/character, odd character parity and LRC with even parity.

c. The standard magnetic format for TTS is 210 bits/inch, 5 bits/character, odd character parity and LRC with even parity.

2. Sentinel characters:

a. The standard start sentinel character for IATA is the percent sign (%).

b. The standard start sentinel character for ABA and TTS is the semi-colon (;).

c. The standard end sentinel character for IATA, ABA and TTS is the question mark (?).

By default, the standard ISO7811 track configurations for magnetic stripe encoding are used by OnGuard:

- Track 1: IATA magnetic format with standard IATA sentinel characters
- Track 2: ABA magnetic format with standard ABA sentinel characters
- Track 3: TTS magnetic format with standard TTS sentinel characters

Using Non-Standard Track Configurations

OnGuard can vary the magnetic format and sentinel characters encoded on each track for some supported printers. The amount of control over the track configuration varies by printer type, and not all printer types can use a non-standard track configuration. Modification to the **ACS.INI** file is necessary to use this special feature. Each printer type has specific instructions for setting up a non-standard track configuration.

Information Specific to Magicard Card Printer Drivers

The following non-standard track configurations are supported for card printers whose card printer drivers are assigned to the type “MagicCard” in the Encoding section of the **ACS.INI** file:

- Track 1: ABA magnetic format with standard ABA sentinel characters
- Track 1: TTS magnetic format with standard TTS sentinel characters
- Track 2: IATA magnetic format with standard IATA sentinel characters
- Track 2: TTS magnetic format with standard TTS sentinel characters
- Track 3: IATA magnetic format with standard IATA sentinel characters
- Track 3: ABA magnetic format with standard ABA sentinel characters

Additional optional parameters must be appended to the appropriate **ACS.INI** Encoding section entry when any of these track configurations are to be used for one of these drivers. They specify which values OnGuard uses for the following track configuration attributes:

- bits/character, listed as **Mode** in the printer driver
- bits/inch, listed as **Density** in the printer driver
- start sentinel character, listed as **Start Character** in the printer driver
- end sentinel character, listed as **Stop Character** in the printer driver

The track configurations default to IATA, ABA and TTS for tracks 1, 2, and 3 respectively. Alternate configurations of these parameters are specified in the **ACS.INI** file in the following syntax: <printer driver>=<print driver type>, <track_1_config>,<track_2_config>,<track_3_config>.

For example: Magicard Card Printer=MagicCard,ABA,TTS,IATA

Note: If fewer than three (3) configurations are specified in the **ACS.INI** file, the default shall be used for the remaining unspecified tracks.

The standard magnetic format attributes (bits/inch, bits/character, character parity, use of an LRC and LRC parity) will be used for each track configuration specified in the **ACS.INI** file. OnGuard uses the current driver settings specified via the printer driver for the remaining track configuration attributes except for coercivity (always specified by OnGuard as “high”).

OnGuard specifies values for the following attributes regardless of whether or not track configurations are specified in the **ACS.INI** file. These attributes must have the default value of “User specify” in the Magicard printer properties:

- Encoding coercivity
- Mode
- Density
- Start character
- Stop character

Information Specific to DNP Magicard (e.g. Prima 4) Printer Drivers

The following non-standard track configurations are supported for card printers whose card printer drivers are assigned to the type “DnpMagicard” in the Encoding section of the ACS.INI file:

- Track 1: NTT magnetic format with standard NTT sentinel characters
- Track 3: NTT magnetic format with standard NTT sentinel characters

Additional optional parameters must be appended to the appropriate ACS.INI Encoding section entry when any of these track configurations are to be used for one of these drivers. They specify which values OnGuard uses for the start sentinel characters and end sentinel characters. Other track configuration attributes (bits/inch, bits/character, character parity, use of an LRC and LRC parity) are specified through the printer driver.

The track configurations default to IATA, ABA and TTS for tracks 1, 2 and 3 respectively. Alternate configurations of the start sentinel characters and end sentinel characters are specified in the ACS.INI file in the following syntax:

<printer driver>=<print driver type>, <track_1_config>,<track_2_config>,<track_3_config>.

For example: CX-D80 U1=DnpMagicard,IATA,ABA,NTT

Note: If fewer than three (3) configurations are specified in the ACS.INI file, the default shall be used for the remaining unspecified tracks.

Information Specific to Fargo/Kodak/JVC Card/Legacy Eltron Card Printer Drivers

The following non-standard track configurations are supported for card printers whose card printer drivers are assigned to the type “Persona” or “GenericISO7811” in the Encoding section of the **ACS.INI** file:

- Track 1: Magnetic format specified for track 1 via the print driver properties with standard ABA/TTS sentinel characters
- Track 2: Magnetic format specified for track 2 via the print driver properties with standard IATA sentinel characters
- Track 3: Magnetic format specified for track 3 via the print driver properties with standard IATA sentinel characters

Additional optional parameters must be appended to the appropriate **ACS.INI** Encoding section entry when any of these track configurations are to be used for one of these drivers. They specify which values OnGuard uses for the start sentinel characters and end sentinel characters. Other track configuration attributes (bits/inch, bits/character, character parity, use of an LRC and LRC parity) are specified through the printer driver.

The track configurations default to IATA, ABA and TTS for tracks 1, 2 and 3 respectively. Alternate configurations of the start sentinel characters and end sentinel characters are specified in the **ACS.INI** file in the following syntax: <printer driver>=<print driver type>, <track_1_config>,<track_2_config>,<track_3_config>.

For example: DTC520_525 Card Printer=Persona,ABA,TTS,IATA

Note: If fewer than three (3) configurations are specified in the **ACS.INI** file, the default shall be used for the remaining unspecified tracks.

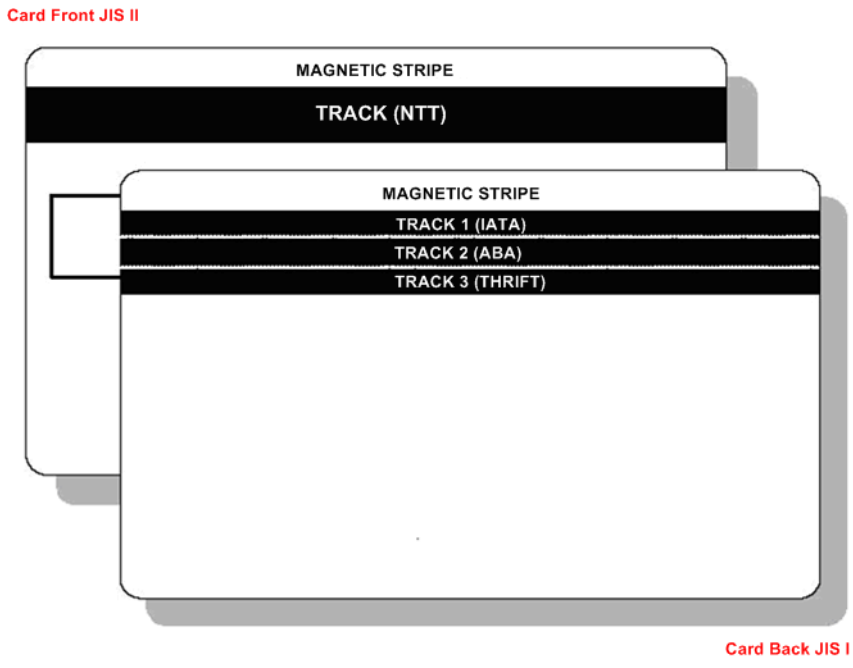
JIS II Encoding (Fargo)

JIS refers to several Japanese Industrial Standards for encoding the Japanese language. JIS II magnetic card encoding standards (JIS X6301, X6302) provide encoding compatibility with the JIS X 0201 Type II cards commonly used in Japan.

The JIS II data format is used to encode the single track on the magnetic stripe located on the front of the Japanese card. The JIS II track is wider than the ISO track (approximately as wide as ISO Tracks 1 and 2).

Notes: The JIS I data formats are the Japanese equivalent to those of ISO/IEC 7811. JIS I uses Track 2.

The JIS II data format is based on the “Roman” character set of JIS X 0201 which is identical to the 7-bit ASCII table except for a few entries representing Japanese kanji characters.



Magnetic Stripe Data Format

Card Type	Track	BPI	Bits/Character	Number of Characters	Character Type
ISO/JIS I	TRACK 1 (IATA)	210	7	79	Alphanumeric
	TRACK 2 (ABA)	75	5	40	Numeric
	TRACK 3 (THRIFT)	210	5	107	Numeric
JIS II	TRACK (NTT)	210	8 (7 bits plus 1 even parity bit per character)	72 (maximum character is 69, plus the start and end sentinels, and an 8-bit LRC character with even parity)	Alphanumeric

Configure a Badge Layout to Encode Data onto a JIS II Magnetic Stripe

Rather than using the magnetic card format to encode the JIS II magnetic stripes, a special text object is used on the front badge layout for specifying both the magnetic encoding command and the JIS II magnetic data.

IMPORTANT: The badge layout that follows is recommended for use with JIS II-capable Fargo printers including the Persona C30, Persona M30, DTC400, DTC550, HDP600, and HDP5000.

Prerequisites:

- MLE support must be enabled.
- The JIS II magnetic encoding mode must be selected in the current Windows user's Printing Preferences for your printer. Click the Start button, then select ***Control Panel*** > ***Printers and Faxes***. Right-click on the printer, then select **Printing Preferences**.

IMPORTANT: Do NOT assign a magnetic card format to any badge type that is going to use this badge layout. It will conflict with the special text object.

In BadgeDesigner, complete the following steps:

1. Add a text object to the badge layout. The size and position of the object does not matter right now.
2. Give the object a name that is indicative of its purpose, such as “JIS II Magnetic Data” or “Amano Magnetic Data.”
3. Set the object's **Text property** to the same data expression you would specify as the track data for a magnetic card format on the Custom Encoding form in the Card Formats folder:
   a. At the beginning, type `~2` where “~2” is track 2 followed by `«{127}»` where “«{127}»” is an ASCII code field with its code set to 127.
   b. Type the data.
   c. At the end, type `«{127}»`.

Example 1: To encode the data for “ABCDEFGHIJKLMNOPQRSTUVWXYZ” (26 characters), set the **Text** property to the following:

~2«{127}»ABCDEFGHIJKLMNOPQRSTUVWXYZ«{127}»

Example 2: To encode the data for the 21 characters of Amano Time and Attendance Data, set the **Text** property to the following (provided you have added a user-defined badge field named “Amano Card Type” with a single character as its length):

~2«{127}»A«’Activate Date’,CDT,”%y%m%d”»000«’Amano Card Type’,F,1L,{48}»«’Cardholder ID’,F,10L,{48}»«{127}»

This would encode the following sequence of characters on a badge with an activation date of “12/25/2007”, an Amano Card Type field value of “G”, and a Cardholder ID of “1234567890”:

A071225000G1234567890

4. Leave the object's **Font** property set to its default value of “Arial 10 pt.”
5. Now move and size the object so that it is large enough to completely display the data expression and also spans, but does not extend beyond the entire width of, the printable page region.
6. Set the object's **Text Foreground Color** property to white so that the contents of the Text object are not displayed during print preview.
7. Ensure the object remains positioned beneath any other object that intersects it. To do this:
   a. Use the Badge Objects list to select the special text object.
   b. From the ***Edit*** menu, select ***Move to Back***.

IMPORTANT: Do not set object’s **Visible** property to “No.” Doing so will cause the object to be completely ignored during printing, and therefore cause no magnetic command or data to be sent to the printer driver.

Information Specific to DataCard Card Printer Drivers

It is not necessary to specify magnetic track configurations in the Encoding section of the **ACS.INI** file to encode magnetic track configurations other than the standard ISO7811 track configurations via DataCard drivers. OnGuard specifies only the data to encode with these drivers and relies upon the magnetic track formats, start sentinel characters and end sentinel characters specified for these printers in the print driver properties.

Information Specific to Zebra (formerly Eltron) Card Printer Drivers

It is not necessary to specify magnetic track configurations in the Encoding section of the **ACS.INI** file to encode magnetic track configurations other than the standard ISO7811 track configurations via a Zebra driver with the type name of “PrivilegeNT.” OnGuard specifies only the data to encode and relies upon the magnetic track formats, start sentinel characters and end sentinel characters specified for the printer in the print driver properties. For legacy Eltron printers with a driver named “PRIV300” or “PRIV400”, refer to section: Information Specific to Fargo/Kodak/JVC Card/Legacy Eltron Card Printer Drivers on page 1446.

Information specific to NiSCA Card Printer Drivers

The encoding of magnetic track configurations other than the standard ISO7811 track configurations is currently not supported for NiSCA card printers. There is currently no way to specify the magnetic track formats, start sentinel characters or end sentinel characters for NiSCA card printers in the print drivers.

Direct Printers with Inline Encoders

Direct printers can be upgraded with various card encoding modules (contact and contactless) as well as for magnetic stripe.

Note: Setup for a printer with an inline proximity encoder, such as the DigiOn24, is different than for a printer with an integrated magnetic encoder in that the inline encoder must be connected directly to the workstation as it does not communicate with the printer.

Configure a Direct Printer for Inline Encoding

Prerequisites:

- Before you install the printer, refer to the Badge Printers Compatibility Chart. To locate the chart, go to Lenel's secure Customer Self Service Center at: https://customer.lenel.com under **Technical Support Tools**. You will need your valid Username and Password.
- Ensure that you have two (2) connections from the printer to the workstation:
  - one (1) for the printer (either USB or parallel)
  - one (1) for the encoder (typically a DB9 serial connection)

To configure a direct card printer for inline encoding, complete the following steps:

1. Install the printer with its supported drivers on a Windows workstation and print a test page to verify functionality.
2. Add the workstation connected to the encoder:
   a. If your encoder is a Magstripe Swipe Reader/Writer, configure it via the Windows printer driver then skip to step 3.
   b. In System Administration or ID CredentialCenter:
      - From the ***Administration*** menu, select ***Workstations***. The Workstations folder is displayed.
      - Select the Encoders/Scanners tab and then click [Add].
   c. On the General sub-tab:
      - In the **Name** field, enter a descriptive name for the encoder/scanner.
      - From the **Workstation** drop-down, select the workstation to which this encoder/scanner is attached.
      - Select the **Device type**. For more information, refer to the Badge Printers Compatibility Chart which cross-references OnGuard versions with supported devices and software.
      - The **Credential technology** field is automatically populated. However, if more than one technology is supported, you can select a different technology from the drop-down.
   d. On the Location sub-tab:
      - Select the **This is an inline device that resides within a card printer attached to this workstation** *<name>* radio button.
      - In the **Card printer** drop-down, select the printer.
      - In the **Encoder station** drop-down, select "Contactless."
   e. On the Communications sub-tab, select values for the fields that display and then click [OK].

Note: If you are configuring a DigiOn24 encoder, ensure **Baud rate** is set to 9600.

3. Create a card format that will contain the data to be encoded on the badge. For more information, refer to Assign an Encoding Format to a Badge Type on page 318.

4. Modify the Badge Type for printing and inline encoding:
   a. From the ***Administration*** menu, select ***Badge Types***. The Badge Types folder is displayed.
   b. Select the badge type in the listing window and then select the Printing sub-tab on the right.
   c. Click [Modify].
   d. In the **Printer to use for this workstation (overrides default)** drop-down, select the printer and then click [OK].
   e. On the Encoding tab:
      - Select a card format. If the card format you want to use is not available in the listing window, add it.
      - Ensure "Always" is selected in the **Inline encode** drop-down
      - Click [OK].

APPENDIX I

Integrating ActivIdentity CMS with OnGuard

The ActivIdentity Card Management System (CMS) handles card management of a individual's smart card for logical access. CMS cards can be "issued" (local issuance or binding for self-enrollment with My Digital ID) from the OnGuard software.

IMPORTANT: If the CMS card is not issued from OnGuard then the card cannot be synchronized with an OnGuard badge.

Once the card is issued, the OnGuard badge is associated with the ActivIdentity card, and any changes to the OnGuard badge record will automatically update the status of the individual's CMS record. If the badge is suspended or revoked in OnGuard, then the person's logical account access in CMS will be suspended.

Note: ActivIdentity Card Management System (CMS) is also known as ActivIdentity Identity Management System (AIMS).

A plug-in is available from Lenel that enables changes in ActivIdentity records to automatically be reflected in the status of the OnGuard badge. The plug-in also allows for event notification in Alarm Monitoring. For more information, refer to ActivIdentity CMS Events Displayed in Alarm Monitoring on page 1462. This plug-in can only be implemented by Lenel's Professional Engineering Services group.

CMS Feature Summary

Feature	Location	Licensed?	Professional Engineering Services required?
Issuance	General OnGuard product	Yes	No
Changes in OnGuard badge state reflected in ActivIdentity CMS credential state	General OnGuard product	Yes	No

CMS Feature Summary

Feature	Location	Licensed?	Professional Engineering Services required?
Changes in ActivIdentity CMS credential reflected in OnGuard badge state	CMS plug-in	No	Yes
CMS event notification in Alarm Monitoring	CMS plug-in	No	Yes

Referenced ActivIdentity Documents

This documentation focuses on the OnGuard side of the ActivIdentity CMS integration. For more information about ActivIdentity, please refer to the following documents that came with your ActivIdentity system:

- ActivIdentity Card Management System (CMS) Operator Guide
- MDIDC (My Digital ID Card) User Portal Guide
- ActivClient Installation Guide
- ActivClient User Guide
- ActivClient Overview

Terminology

ActivClient. The ActivIdentity client software, which must be installed on all ID CredentialCenter workstations and user workstations.

ActivIdentity Generated Client certificate. A certificate that may be generated by the ActivIdentity system setup that contains the first operator credentials. It can be used to authenticate with the CMS as an operator so that additional operator and user credentials can be issued. After being used to create another operator's certificate, the ActivIdentity Generated Client should be removed from the system for security purposes.

Binding. An option that may be used when enrolling badges in the OnGuard/ActivIdentity system that links the card to the user in CMS and allows the user to personalize the card using My Digital ID. Binding does not personalize the card (no data is written to the card).

Certificate. A file or electronic document used to authenticate as an operator with the CMS server in order to enroll and encode badges (if local issuance is used).

CMS. Card Management System. Typically provides management for card issuance, the card life cycle, and cardholder data for various card types.

Local issuance. An option that may be used when enrolling badges in the OnGuard/ActivIdentity system that personalizes the smart card (writes data to the card).

Logical access. Access control by which a system grants or restricts the right to access computer applications, networks, and data. Cardholders with the appropriate clearances or permissions are provided with smart identification (ID) cards that verify their rights and privileges. Once presented, scanned, or inserted into readers, these credentials permit access to secure information which encompasses the data and intellectual property residing on computer networks.

Smart card logical access allows organizations to issue a single ID card that supports logical access, physical access, and secure data storage, along with other applications.

Additionally, logical access controls can be used to limit user access only to information which is appropriate for them. Logical access controls are often built into the operating system, or may be part of the "logic" of application programs or utilities, such as Database Management Systems. Logical access may also be implemented in add-on security packages that are installed into an operating system such as CMS.

Operator. In CMS terminology, a trusted individual who has administrative rights to perform critical operations on the CMS that cannot be done by a user. Each operator's permissions are defined by his or her assigned role.

Physical access. Access control by which a system grants or restricts the right to access buildings and facilities in order to secure areas of the workplace such as parking garages, manufacturing facilities, and research and development laboratories.

PKI. Public Key Infrastructure. A set of policies, processes, and technologies used to verify, enroll, and certify users of a security application. PKI uses public key cryptography and key certification practices to secure communications, including the Certificate Authority (CA), key directory, and management.

Using ActivIdentity CMS with OnGuard

Basic integration between ActivIdentity CMS with OnGuard enables you to:

- Perform local-issuance or binding for self-issuance of ActivIdentity smart cards, including PIV cards, during the badge issuance process in ID CredentialCenter.
- Propagate OnGuard badge life cycle events, such as badge encoding, activation, deactivation, and deletion to CMS.

If the optional CMS plug-in is used, you may also do the following:

- Propagate ActivIdentity CMS card life cycle events such as suspending, resuming, or terminating a card to the OnGuard software.
- Receive various ActivIdentity CMS events in Alarm Monitoring.

Badging operators using CMS with OnGuard will likely need to handle the following scenarios:

- Encode/Bind a CMS Card on page 1464
- Encode/Bind a PIV Card on page 1465
- Modify Badge Status on page 1467
- Delete a Badge on page 1467
- Delete a User or Cardholder on page 1467
- Manage Lost Badges on Systems Integrated with ActivIdentity CMS on page 1468
- Revoke a PKI Credential in ActivIdentity CMS on page 1468

Licensing Requirements for ActivIdentity CMS

Encoding an ActivIdentity CMS card in OnGuard requires the “ActivIdentity CMS integration” and “Maximum Number of ActivIdentity CMS Badges Encoded” licenses. Each time a badge is synchronized (encoded) with ActivIdentity CMS, an internal counter is incremented. The number of cards that have been encoded or bound for self-enrollment is displayed on the ActivIdentity CMS form (***Logical Access*** > ***ActivIdentity***). Once the counter reaches the maximum value specified in the license, you will receive notification and all future attempts to encode will fail until additional instances are purchased.

Setting up the OnGuard ActivIdentity CMS Client Computer

On the CMS client computer, do the following:

1. Install the OnGuard software. Refer to the Installation Guide for more information.
2. Install the OnGuard license. Refer to Install the OnGuard License on page 1456 and the Installation Guide for more information.
3. Install the ActivClient software. You must install “ActivClient” on any workstation that will be used to manage CMS badges. For more information, refer to Install ActivClient on page 1456.
4. Configure ActivIdentity CMS in the OnGuard software. For more information, refer to Configure ActivIdentity CMS in OnGuard on page 1457.

Install the OnGuard License

To use ActivIdentity CMS, you must have an OnGuard license that enables use of the ActivIdentity feature and specifies the number of card issuances (local or with self enrollment) purchased. For more information about the license, refer to Licensing Requirements for ActivIdentity CMS on page 1456. For specific information on how to install the OnGuard license, refer to the Installation Guide.

Install ActivClient

The ActivClient software allows OnGuard and ActivIdentity CMS to work together. You must purchase “ActivClient” from ActivIdentity and then install it in the following locations:

- On any ID CredentialCenter workstation that will be used to issue or manage CMS badges.
- On each user workstation, so the workstation can interact with issued credentials.

ActivClient is required to be running on the ID CredentialCenter workstations and user workstations in order to:

- Log onto a computer using an issued card
- Issue and manage cards

Note: Once ActivClient is installed, it automatically starts up and runs when Windows starts up.

To install ActivClient, refer to the ActivClient Installation Guide for detailed instructions.

Configure ActivIdentity CMS in OnGuard

To accomplish this integration, complete the following configuration steps in the OnGuard software in the order listed:

1. Verify User Permissions on page 1457
2. Add a CMS Connection on page 1457
3. Verify Connectivity to the Selected CMS on page 1458
4. Configure ActivIdentity Cardholder Options on page 1458
5. Add a CMS Smart Card Format on page 1459
6. Add a Badge Type for CMS on page 1459
7. Configure a Workstation for CMS on page 1461
8. Configure an Encoder for CMS on page 1461
9. Add DataConduIT Sources for ActivIdentity (CMS Plug-in Users Only) on page 1462

Verify User Permissions

Verify that the user who will perform each of the following tasks has the necessary user permissions:

- Add, modify, or delete a CMS connection

  To perform any of these functions, the system permission group assigned to the user must have the respective CMS system permissions. These are configured from System Administration or ID CredentialCenter in ***Administration*** **>** ***Users*** > System Permission Groups tab > Users, Directories, Logical Access sub-tab > Logical Access category.
- Bind/encode a CMS badge

  In order to bind/encode a CMS badge, the user must have permission to encode badges. This is configured from System Administration or ID CredentialCenter in ***Administration*** **>** ***Users*** > Cardholder Permission Groups tab > Badge sub-tab > **Encode badges** check box.
- Manage badges bound to CMS cards

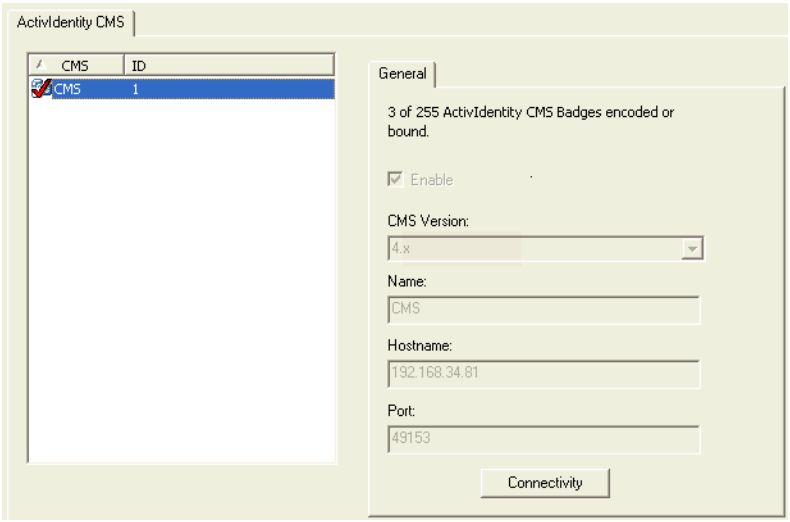
  The OnGuard user managing badges bound to CMS cards must be a registered operator in CMS with the appropriate permissions. The CMS operator authenticates to CMS using a digital certificate. CMS operator permissions are defined by a Role in CMS. For more information, refer to the ActivIdentity Card Management System (CMS) Operator Guide.

Add a CMS Connection

Note: Refer to Verify User Permissions on page 1457 for the user permissions required to perform this task.

1. From the ***Logical Access*** menu in System Administration or ID CredentialCenter, select ***ActivIdentity***. The ActivIdentity CMS folder opens.
2. Click [Add].
3. From the **CMS Version** drop-down, select the major version of the CMS server.
4. In the **Name** field, enter a unique name that will be used to identify the CMS system in the OnGuard software.
5. In the **Hostname** field, type either the IP address or the full computer name of the machine hosting the CMS.
6. In the **Port** field type the port on which the CMS is listening for requests. Check the CMS Install Guide for the port number; historically it has been 49153.

7. If the CMS server is online and you wish to connect to it, leave the **Enable** check box selected. If not, deselect the **Enable** check box.
8. Click [OK]. Your CMS entry should resemble the following:



9. Verify connectivity to the selected CMS. For more information, refer to Verify Connectivity to the Selected CMS on page 1458.

Verify Connectivity to the Selected CMS

SSL protocol with mutual authentication is used during interactions between OnGuard and CMS. In order to connect to ActivIdentity CMS to perform card issuance and management, an operator must have valid CMS operator's credentials (certificates) with the appropriate roles. Upon receiving requests for operations from OnGuard, CMS verifies that the role assigned to the operator's credential is allowed to perform the operations.

1. On the ActivIdentity CMS form (***Logical Access > ActivIdentity***), select the CMS connection you want to test. If the connection does not exist yet, you may add it and test the connection while adding it.

Note: The **Enable** check box must be selected for the CMS server connection in order to enable the [Connectivity] button. If it is not, connectivity cannot be tested.

2. Click [Connectivity].
3. The Choose a digital certificate window opens. Select a CMS operator's certificate. If no certificates are available then you will have to install one. Refer to the ActivClient Installation Guide for instructions on installing an operator's certificate.

Note: The OnGuard computer that is connecting to the CMS server must have the operator's certificate installed to connect successfully. If necessary, validate that the root certificate path is trusted.

Configure ActivIdentity Cardholder Options

In the Cardholder Options folder, you configure the Cardholder deletion behavior to define what happens to a logical user account when a cardholder is deleted in the OnGuard software. The available options are:

- Do nothing to the directory user account (This is the default option.)
- Delete the directory user account
- Terminate (delete) all of a user's logical badges

To configure ActivIdentity Cardholder Options:

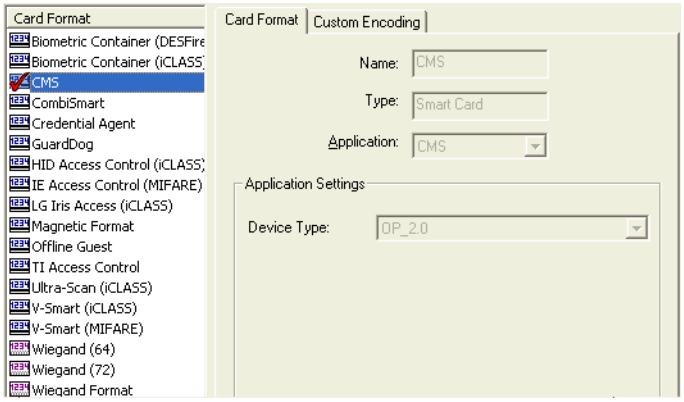
1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Cardholder Options***.
2. Click the Logical Access tab.
3. Click [Modify].
4. In the **Cardholder deletion behavior** drop-down, select the desired behavior.
5. Click [OK].

Add a CMS Smart Card Format

1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Card Formats***.
2. Click [Add].
3. The Choose Card Format Type dialog opens. Select "Smart Card", and then click [OK].
4. In the **Name** field, type a unique name for the new card format.
5. In the **Application** field, select "CMS."

Note: In the **Device Type** field, the CMS device type is pre-selected to "OP_2.0".

6. Click [OK]. Your card format should resemble the following:



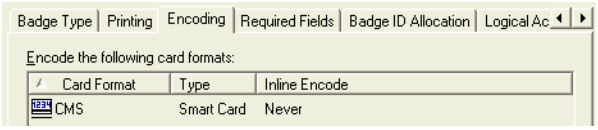
Add a Badge Type for CMS

In order for a badge to be encoded with CMS or be subject to lifecycle events, the badge's badge type must be configured to be registered with ActivIdentity. To do this:

1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Badge Types***.
2. Modify an existing badge type or add a new badge type. This badge type must have the following settings:
   a. On the Badge Type tab:
      1) If you are adding a badge type, in the **Class** drop-down, select "Standard."
   b. On the Encoding sub-tab:

2) Click [Add].

3) The Add Card Formats dialog displays. Select the CMS card format you created in Add a CMS Smart Card Format on page 1459.



Note: Any card format may be linked to a badge type.

4) Click [OK].

c. On the Logical Access sub-tab, complete the following steps:

5) Select the **Register badge with ActivIdentity** check box if you wish to do so.

6) Select an **Issuance action**. Choices include:

Local issuance - personalizes the smart card (writes data to the card).

Issuance with self-enrollment (binding) - does not personalize the card (no data is written to the card). Binding only links the card to the user in CMS and allows the user to personalize the card using CMS's My Digital ID.

Notes: To be able to perform Issuance with self-enrollment (binding) and Local issuance, simply add two badge types - one for each action. The same card format may be linked to both badge types.

For CMS version 4.0/4.1, Issuance with self-enrollment (binding) also includes the submission of a badge production request (to define the policy and other information required for self-enrollment).

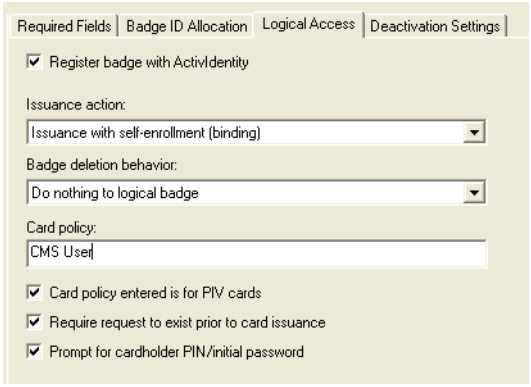
7) Select a **Badge deletion behavior**. Choices include:

Do nothing to logical badge

Suspend logical badge

Terminate logical badge

8) In the **Card policy** field, type the CMS card policy that will define what applications and credentials can be issued to bound cards by CMS.



IMPORTANT: Take care to enter the policy name correctly in the **Card policy** field. This must be the same name that is used in CMS, and is case-sensitive.

9) Select the **Card policy entered is for PIV cards** check box if the Card policy entered is for the issuance of a PIV card.

Note: When this option is selected, fingerprint verification is performed immediately after the card is encoded. For more information, refer to Encode/Bind a PIV Card on page 1465.

10) Select the **Force request to exist prior to card issuance** check box if the production request will be submitted by a third party system before OnGuard performs the issuance.

Notes: For CMS version 4.0/4.1: If this option is not selected, then OnGuard will submit the production request and immediately execute it. However, to ensure compliance with FIPS standards, it is recommended that the production request comes from CMS. **Force request to exist prior to card issuance** must be selected.

For CMS version 3.8: OnGuard always submits the production request. Therefore, ensure that **Force request to exist prior to card issuance** is deselected.

11) Click [OK].

Configure a Workstation for CMS

You must first add a workstation before you can add an encoder. To do this, select ***Workstations*** from the ***Administration*** menu in System Administration or ID CredentialCenter. Refer to Add a Workstation Entry on page 381 for complete instructions.

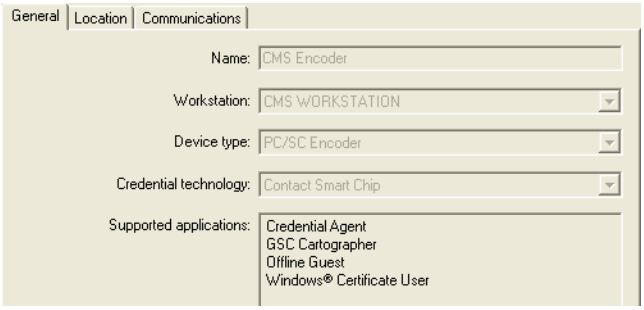
Configure an Encoder for CMS

Prerequisites:

- A workstation must be configured in the OnGuard software. For more information, refer to Configure a Workstation for CMS on page 1461.
- The encoder must be attached to the workstation. (If it is not, you can configure this later, but it must be configured in order for the CMS integration to work.)

To issue CMS badges, you must configure an encoder in the OnGuard software. Any supported PC/SC encoder configured for use with the CMS workstation can be utilized during the issuance of the CMS badge. To configure an encoder:

1. From the ***Administration*** menu in System Administration or ID CredentialCenter, select ***Workstations***.
2. Click the Encoders/Scanners tab.
3. Click [Add]. For complete instructions, refer to Configure an Inline or Standalone Encoder/Scanner on page 388. For CMS integration, you must select the following settings:
   a. On the General tab, be sure to enter a **Name** and select “PC/SC Encoder” in the **Device type** field.



b. On the Communications sub-tab, select the correct **PC/SC device**.
   - If you are at the workstation and the encoder is attached, simply select it in the drop-down list.
   - If you are not at the workstation, you cannot select the PC/SC device yet. You can add the encoder record, but an information message will be displayed, and you will need to go to the workstation and configure this later.

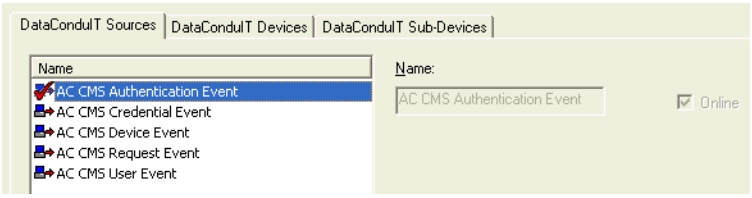
Add DataConduIT Sources for ActivIdentity (CMS Plug-in Users Only)

This procedure should only be performed on systems that will be using the optional CMS plug-in. In order to receive CMS events in Alarm Monitoring, you must add DataConduIT Sources in the OnGuard software. This is done in System Administration by selecting ***DataConduIT Sources*** from the ***Additional Hardware*** menu. For complete instructions, refer to Add a DataConduIT Source on page 1170.

From the DataConduIT Source items in the table, add those which describe the type of CMS events you wish to monitor:

DataConduIT Sources name	CMS event
AC CMS Device Event	Device Related
AC CMS User Event	User Related
AC CMS Request Event	Request Management Related
AC CMS Credential Event	Credential Management Related
AC CMS Authentication Event	Authentication Related

Your configured DataConduIT Sources should look like the following:



ActivIdentity CMS Events Displayed in Alarm Monitoring

Depending on which DataConduIT Sources you have configured, notification of different CMS events will be displayed in Alarm Monitoring and logged.

Several CMS events are listed in the following tables. (For a complete list of CMS events, refer to the ActivIdentity documentation).

CMS Event	Description
Device Related	
ActivateDevice	This event is generated upon the logical activation of a card in CMS

CMS Event	Description
CardIssuance	Card encoding is complete. This event is generated after a smart card is issued to a cardholder/user:
CardBind	Card binding is complete. This event is generated after a card has been assigned to a user.
CardUnbind	A card has been unbound. This event is generated after a card is unassigned from a cardholder/user.
CardRecycle	This event is generated before a card is recycled.
Replace	This event is generated after a request for a replacement card is submitted.
RequestUnlock	This event is generated when a card is abut to be unlocked.
ResumeDevice	This event is generated after a card is resumed.
SuspendDevice	This event is generated after a card is suspended.
Terminate	This event is generated after a card is terminated.
User Related	
CreateUser	This event is generated when a user is added to the directory with CMS.
DeleteUser	This event is generated when a cardholder/user is deleted from the directory with CMS.
TerminateUser	This event is generated when a cardholder/user is terminated.
WriteOperator	This event occurs when a CMS operator is enrolled or when the definition of an operator is updated.
DeleteOperator	This event occurs when a CMS operator is deleted.
Request Management Related	
WriteRequest	This event is generated just after a request is created.
ApproveRequest	This event is generated when a request is approved. **Note:** Notification occurs only if there is formal approval of the request. There is no event when the request is approved automatically by the system (for example unlock or post-issuance requests).
DenyRequest	This event is generated when a request is denied.
DeleteRequest	This event is generated when a request is deleted by the system, after the request is successfully processed (for example, after an unlock request is executed).
CancelRequest	This event is generated when a request is cancelled.

CMS Event	Description
Credential Management Related	
CreateCredential	This event is generated before execution of a request to create a credential, just before it is sent to the credential provider.
CredentialIssued	This event is generated when a credential is issued.
CredentialRequest	This event is generated when a credential issuance request is created, just before it is sent to the repository, such as the CA server.
CertHold	This event is generated after a credential is suspended.
CertResume	This event is generated after a credential is resumed.
CertRevoke	This event is generated after a credential is revoked. For more information, refer to Revoke a PKI Credential in ActivIdentity CMS on page 1468.
Authentication Related	
AuthenticateUser	This event is generated when a user logs into My Digital ID Card.
AuthenticateOperator	This event is generated when an operator logs into the CMS Operator Portal.

Badge Operations Using ActivIdentity CMS with OnGuard

The following procedures can be performed when using ActivIdentity CMS with OnGuard.

Encode/Bind a CMS Card

Note: Refer to Verify User Permissions on page 1457 for the user permissions required to perform this task.

Prerequisite: Before performing this procedure, you must have an encoder properly configured in the OnGuard software. Any supported PC/SC encoder configured for use with the CMS workstation can be utilized during the issuance of the CMS badge. For more information, refer to Configure an Encoder for CMS on page 1461.

To bind/encode a CMS card:

1. Log into the ID CredentialCenter workstation, and then log into OnGuard.
   - If you log into the workstation using your smart card, then the certificate is automatically copied to the computer's personal store.
   - If you log into the workstation by typing your user name and password, you will need to manually install the certificate that has been granted operator's privileges in the ActivIdentity system before you can authenticate with the server and perform encoding.
2. From the ***Administration*** menu, select ***Cardholders***.

3. Search up an existing cardholder and click [Modify], or add a new cardholder by clicking [Add].
4. On the Badge tab:
   - In the **Badge type** field, select the badge type that you created in Add a Badge Type for CMS on page 1459.
   - Be sure the **Status** is "Active".
   - Click [OK].
5. From the Logical Access tab, link the user's logical account to the cardholder by doing the following:
   a. Select the **Issuing CMS**. This is the CMS that the user exists in. It is also the CMS that is connected to when issuing the badge to the cardholder.
   b. Enter the **User ID**, which is the cardholder's logical user account name.
   c. Click [OK].

Notes: The Cards listing window lists all cards/badges that have been encoded or bound to the cardholder. If the check box **Update list from server** is selected, then the list will also display badges which were issued to users outside of OnGuard.

Badges issued to users outside of OnGuard cannot be linked to a physical badge and thus do not support life cycle management.

Additional operations on the badge (such as resuming, suspending, terminating, or unlinking) can be performed by right-clicking on an entry in the list.

6. Return to the Badge tab and click [Encode]. The Encode Badge window opens.
   a. Select the CMS card format you created in Add a CMS Smart Card Format on page 1459.
   b. Select the encoder that you configured in Configure an Encoder for CMS on page 1461.
   c. Click [Encode].

   If badge issuance is being used, the card is encoded based on the Card policy defined.

   If badge binding is being used, the badge is bound to the user. This behavior is dependent on the **Issuance action** configured in step 6 in Add a Badge Type for CMS on page 1459.

   The card and issuing/binding CMS information is then captured.

Note: A system check will be performed to validate the status of the badge being encoded/bound. For more information, refer to Issuance Validation on page 1466.

Encode/Bind a PIV Card

The issuance of PIV cards using OnGuard is almost identical to the issuance of non-PIV cards. However, PIV cards may contain several data elements such as fingerprints, facial images, the Cardholder Unique Identifier (CHUID), as well as multiple certificates that do not exist in OnGuard. Therefore, all data that will be encoded on the PIV card must be sent to CMS prior to PIV card issuance.

IMPORTANT: The Badge Type used for PIV card issuance must specify that the Card policy entered is for PIV cards. For more information, refer to Add a Badge Type for CMS on page 1459.

Verify Fingerprint(s)

For PIV card issuance, FIPS 201 Specifications require 1:1 fingerprint verification prior to issuing a card to the cardholder/visitor. After you have personalized the PIV card, the Verify Fingerprint(s) dialog is displayed allowing you to verify the cardholder's fingerprint against those just encoded on the card. For more information, refer to Verify Fingerprint(s) Dialog on page 96.

1. Follow the on-screen prompts provided in the status box below the fingerprint image. You will be guided through the process of capturing the fingerprint(s).
2. From the **Capture Device** drop-down select the device you will use to capture the fingerprints.
3. When prompted, the cardholder presents his/her finger to the capture device.
4. Click [Capture].
5. If the fingerprints match, a successful issuance is registered with OnGuard. However, if fingerprint verification fails, the card is terminated and recycled.

Note: If the PIV card contains a facial image, it is displayed with the captured fingerprint image for additional verification of the cardholder.

6. To stop the capture operation, click [Abort].

Issuance Validation

When you encode or bind a badge, the state of the badge being encoded or bound is checked by the system to ensure it is in a valid state for issuance.

Badge Status?

If the badge is not in a valid state for issuance, then the various operations are executed automatically in an attempt to recover the badge into a valid state. A badge cannot be encoded or bound unless it is in such a state.

The following table lists the operation that will take place when the card is in a given state:

Badge status	Operation
Available: The badge is in a valid state for encoding/ binding.	No operation needed as the badge is in a valid state for issuance.
Assigned: The badge is already bound to a user for self-issuance.	The operator is prompted to unbind the badge to return the card to the available state. **Note:** In the case of CMS 4.0/4.1, the issuance request for bound badges is also cancelled.
Issued: The badge is already issued and assigned to a user.	The operator is prompted to terminate the card. If the badge is terminated, it will automatically be recycled, returning the badge to the available state.
Produced: The badge was issued to a user but not assigned (it was not recycled).	The badge is automatically recycled, returning it to the available state.

Badge status	Operation
Invalid: The badge is not in an valid state (it has been suspended, forgotten, damaged, stolen, or lost).	An error is reported and execution stops. The badge cannot be issued or bound to with OnGuard unless it is recovered to a valid state outside of OnGuard.

Badge Already Issued to the Cardholder?

After verifying the status of the card, if the status is available or returned to available, the system checks the status of the cardholder. If the cardholder already has an active card, then the operator is allowed to terminate the active card and continue encoding or binding the new card.

Modify Badge Status

When the status of a badge is changed in the OnGuard software, the change is propagated in CMS. The following describes what happens in the CMS system:

- Badge status is changed from “Active” to an inactive state such as “Lost” or ‘Returned”

  All credentials stored on the CMS badge are suspended.

Note: If a bound badge has not been issued using the self-issuance process, this operation will cause an error because the card is not in a “suspendable” state.

- Badge status is changed from an inactive state to “Active”

  All credentials stored on the user’s suspended badge are reactivated.

Note: If a bound badge has not been suspended, this operation will cause an error because the badge is not in a “resumable” state.

Delete a Badge

Depending on how **Badge deletion behavior** is configured, when you delete a badge in OnGuard, one of the following operations place in CMS:

- No action is taken on the logical badge.
- The user’s logical badge is suspended.

Note: If a bound card has not been issued using the self-issuance process, the suspend operation will cause an error because the card is not in a “suspendable” state. In this case, OnGuard should send an Unbind request to CMS.

- The user’s logical badge is terminated (unbound) and, if there are any, the credentials stored on the card are revoked.

For more information, refer to Add a Badge Type for CMS on page 1459.

Delete a User or Cardholder

Depending on how the **Cardholder deletion behavior** is configured, when you delete a user or cardholder in OnGuard, one of the following operations takes place in CMS:

- No action is taken to the directory user account.
- The directory user account is deleted.

- All of the logical badges assigned to the user in CMS are terminated or unbound.

For more information, refer to Configure ActivIdentity Cardholder Options on page 1458.

Manage Lost Badges on Systems Integrated with ActivIdentity CMS

If a cardholder loses their badge and your OnGuard system is integrated with CMS:

1. Log into the ID CredentialCenter workstation, and then log into OnGuard.
   - If you log into the workstation using your smart card, then the certificate is automatically copied to the computer's personal store.
   - If you log into the workstation by typing your user name and password, you will need to manually install a credential (generally a certificate) that has been granted operator's privileges in the ActivIdentity system before you can authenticate with the server and perform encoding.
2. From the ***Administration*** menu, select ***Cardholders***.
3. Search up the cardholder whose badge is lost.
4. On the Badge tab:
   a. Click [Modify].
   b. In the **Status** field, select "Lost".
   c. Click [OK]. The event will automatically be propagated to CMS, and all credentials stored on the CMS card will then be suspended.

Revoke a PKI Credential in ActivIdentity CMS

If you are a CMS Administrator, you may revoke a PKI credential using the CMS portal. If you do this (and the ActivIdentity CMS plug-in is installed), a "PKI Credential Revoke" event is sent to Alarm Monitoring. For more information, refer to ActivIdentity CMS Events Displayed in Alarm Monitoring on page 1462.

APPENDIX J

Intrusion Command

Enhancements made to the LNL-CK reader now make it possible to arm and disarm alarm mask groups via the LNL-CK device itself.

Intrusion Command Overview

Once properly configured in System Administration, cardholders with the proper permissions are able to arm and disarm alarm mask groups using the LNL-CK reader.

The cardholder with proper permissions who has been granted access at the reader will be able to enter the command string for this new command followed by a two-digit ID of the alarm mask group they want to arm and disarm.

For example, if the user command code is 300, the cardholder would enter (after being granted access) “*30004#” where “300” is the selected command string and “04” is the alarm mask group ID.

To configure this new feature follow the steps below:

1. Configure the System/Segment User Commands on page 1469
2. Configure the Access Levels on page 1470
3. Configure the Reader on page 1470
4. Arming and Disarming from the LNL-CK Reader Using Global Permission Control Only on page 1471

Configure the System/Segment User Commands

1. In System Administration, select the ***Administration*** > ***System Options*** menu option, and select the User Commands sub-tab.

Note: If your system is segmented the User Commands sub-tab can be found in the ***Administration*** > ***Segments*** menu option on the Segments tab.

2. On the User Commands sub-tab select the **Global Permission Control Only** or **Advanced Permission Control** option from the **Intrusion command configuration** drop-down box.
3. Select the Intrusion command code you wish to use. This can be any 3 to 6 digit number. The cardholder enters this number as part of the command string. For example, if the command code is 123, the cardholder would enter "*12304#" where "123" is the selected command code.

Note: The command code can not match the command code that is used by the extended held command code.

Configure the Access Levels

In System Administration, go to the ***Access Levels*** menu option, and click the Access Levels tab.

1. Select the Access Level you wish to have intrusion command authority.
2. Click [Modify].
3. Select the appropriate readers and timezones.
4. Select the **Global Permission Control Only** or **Advanced Permission Control** option from the **Intrusion command configuration** drop-down box.

Notes: Based on what option you choose from the **Intrusion command configuration** drop-down box the LNL-CK will act differently when there are more than one zone in a fault condition.

If you choose **Global Permission Control Only** the cardholder is shown the first device by name on the LNL-CK screen indefinitely with no additional prompting. The cardholder must continue to press 4 on the keypad to view the other devices.

If you choose **Advanced Permission Control** the cardholder is shown the first device by name for 2-3 seconds before it automatically advances to the next. The cardholder may also press 4 on the keypad to immediately view the other devices.

5. Click [OK].
6. Configure the Reader

Configure the Reader

1. In System Administration, go to the ***Access Control*** > ***Reader*** menu option, and click the Reader sub-tab.
2. Select the reader you wish to add the intrusion command to.
3. Click [Modify].
4. Select the **Allow Intrusion Commands** check box.
5. Click [OK].

Note: While theoretically any reader can be used to arm and disarm alarm mask groups this feature is only truly useful with the LNL-CK reader because of its display output.

Arming and Disarming from the LNL-CK Reader Using Global Permission Control Only

1. Once the cardholder who has the correct permissions is granted access they are able to enter a command string into the reader.
2. start by pressing the "*" button. On the LNL-CK this is represented with the arrow key.
3. Follow it by the 3 to 6 digit command code you entered in the user Command sub-tab.
4. Follow that by the 2 digit ID of the particular alarm mask group you wish to arm or disarm.

Note: You can find the ID number in System Administration by going to the Alarm Mask Group sub-tab in ***Access Control > Groups***. There is an ID column in the Alarm Mask Groups listing window. Remember if the ID is a single digit preface it with a zero (0). For example, an ID of 1 would be entered as 01.

5. End the command string by entering the "#" key. On the LNL-CK this is represented with the "Command" key.
   - If the alarm mask group you've selected is currently armed you will be prompted to press "1" to disarm it.
   - If the alarm mask group is currently disarmed and no points are active you will be prompted to press "2" to arm it.
   - If the alarm mask group is disarmed but there are points active you will receive a "NN zones faulted" display where "NN" is the number of points active. You can scroll through these active points by pressing "4". once all the points have been displayed you can press "3" to force-arm the alarm mask group.

Arming and Disarming from the LNL-CK Reader Using Advanced Permission Control

1. Start by pressing the "*" button. On the LNL-CK this is represented with the arrow key.
2. Follow it by the 3 to 6 digit command code you entered in the user Command sub-tab.
3. Follow that by the 1 digit of the particular command you selected.
4. End the command string by entering the "#" key. On the LNL-CK this is represented with the "Command" key.
5. Follow instructions displaying in the LNL-CK LCD.

APPENDIX K

Lenel ILS (Integrated Locking Solutions)

OnGuard allows you to set up and operate several Lenel locking solutions including ILS Integra, ILS offline, and ILS wireless locking systems. For more information, refer to the ILS Integra Locking System Overview on page 1475 and ILS Offline/Wireless Locking Systems Overview on page 1491.

IMPORTANT: When ILS locks are installed in the doors, they are pre-configured with factory settings. The lock information (locking plan) is then configured in OnGuard and downloaded to the XPP or Lenel ILS Mobile Configurator portable device that is used to initialize the locks with the lock settings. For more information, refer to the Lock Configuration section in the ILS Lock Operation Guide.

The vocabulary used:

Access Control Card Formats. A set of attributes that describe to the lock how to validate integrity and parse the access control data retrieved from the credentials. Access control card formats include ISO magnetic tracks (1,2, and 3), Wiegand, Integra, etc.

For more information, refer to Lock Card Formats on page 1499.

ActiveSync. A data synchronization program developed by Microsoft for use with its Microsoft Windows line of operating systems. It provides users of Microsoft Windows a means of transporting information between their desktop computer and a mobile device, such as a Mobile Configurator, mobile phone, or any other portable devices that support the ActiveSync protocol. ActiveSync is available as a free download from Microsoft's web site.

ACU. Refers to the Access Control Unit. The ILS wireless lock contains two (2) micro-controllers (the ACU and WLM) and a reader unit. Firmware for the lock controllers and reader can be downloaded from Alarm Monitoring. For more information, refer to the Alarm Monitoring User Guide.

ADA. Americans with Disabilities Act. In order to be ADA-compliant, extended strike and extended open time is assigned to cardholders with disabilities who require it. The ADA information is configured on the Wiegand card format form. For more information, refer to Add a Wiegand Card Format on page 257.

AFC. Refers to Alternative Fire Code that is also known as Ontario Fire Code 3.4.4.5. This mode requires presentation of the card to relock the door upon exit.

Audit trail. A log of event information that is recorded stored at the lock. “Audit” is used interchangeably with “event” in this document.

Heartbeat. A signal transmitted by the lock’s radio module (WLM) to the Wireless Gateway periodically indicating to the Wireless Gateway that the communications link between the Wireless Gateway and the lock is open. Heartbeat frequency is specified by a parameter stored in the lock.

AWID. AWID is the manufacturer of secure identity solutions including antenna, RF, and communication systems. ILS proximity locks support AWID Prox credentials based on 125 kHz RFID card technology.

CSN. Refers to Card Serial Number. CSN card format types (ISO 14443 and ISO 15693) are used for credential identification. Each smart card contains a Unique permanent Identification Number (UID). This UID is also referred to as the Card Serial Number (CSN). The reader uses a compatible credential method to access the access control data encoded on the card.

HID. HID Global is the manufacturer of secure identity solutions and contactless smart card technology for physical access control. ILS proximity locks supports HID Prox is based on 125 kHz RFID card technology; ILS iCLASS locks support HID iCLASS credentials based on 13.56 MHz RFID technology.

iCLASS. 13.56 MHz read or write contactless smart card technology that is compliant with ISO 15693. For more information, refer to Smart Card CSN Card Format on page 278.

ILS. Refers to Lenel Integrated Locking Solutions.

LED. Refers to Light Emitting Diode.

MC. Refers to the Lenel ILS Mobile Configurator. Use this portable device to initially configure and manage ILS offline and ILS wireless locks. The MC allows you to initialize, download card holders, download and upload events, download lock scheduling information, download firmware updates, and run lock diagnostics. You can also use the MC to unlock the lock and change reader modes as needed.

Offline locks. Describes the standalone locks (ILS Integra and ILS Offline).

Configurator adapter. The Mobile Configurator communicates with the ACU via the Configurator power adapter. The Configurator adaptor can be used to provide auxiliary power to the ILS offline and ILS wireless locks in case the battery is low or has no power.

PP. Refers to Portable Programmer also known as the “Mobile Configurator.”

RF. Refers to Radio Frequency.

RTC. Refers to Real-time Clock.

Smart Card Formats. This card format describes how to retrieve access control data from the smart card credential and pertains to iCLASS locks only.

For more information, refer to Lock Card Formats on page 1499.

WAP. Acronym for a Wireless Access Point device that is also referred to as the ILS Wireless Gateway.

Wireless Gateway. This is an ILS-specific Wireless Access Point (WAP) device; not a common access point. The ILS Wireless Gateway is used to communicate with its associated locks on the 900Mhz frequency range.

WLM. Refers to the Wireless Lock Module, also known as the radio module, in the ILS wireless lock. Firmware for this module and the lock reader can be downloaded from Alarm Monitoring. For more information, refer to the Alarm Monitoring User Guide.

WMC. Refers to the WAP Main Controller micro-controller. Firmware for this controller can be downloaded from Alarm Monitoring. For more information, refer to the Alarm Monitoring User Guide.

WWC. Refers to the Wireless WAP Module micro-controller. Firmware for this controller can be downloaded from Alarm Monitoring. For more information, refer to the Alarm Monitoring User Guide.

XPP. Refers to Extended Portable Programmer. Use this portable device to initially configure and manage the ILS Integra locks.

ILS Integra Locking System Overview

OnGuard allows you to set up ILS Integra locking systems using Integra CT30 offline locks (commonly referred to in OnGuard as doors) and Integra offline controllers (XPP portable programmers) which are treated as access panels by OnGuard.

In Integra offline lock configurations, OnGuard acts as a front end to the data transferred between OnGuard and the Integra offline locks via the XPP.

IMPORTANT: For more information, refer to Configure an ILS Integra Lock System on page 1480.ILS readers (locks) do not support assigning an access level to a cardholder (badge) if that access level contains a lock that is in an access level already assigned to the cardholder (badge).

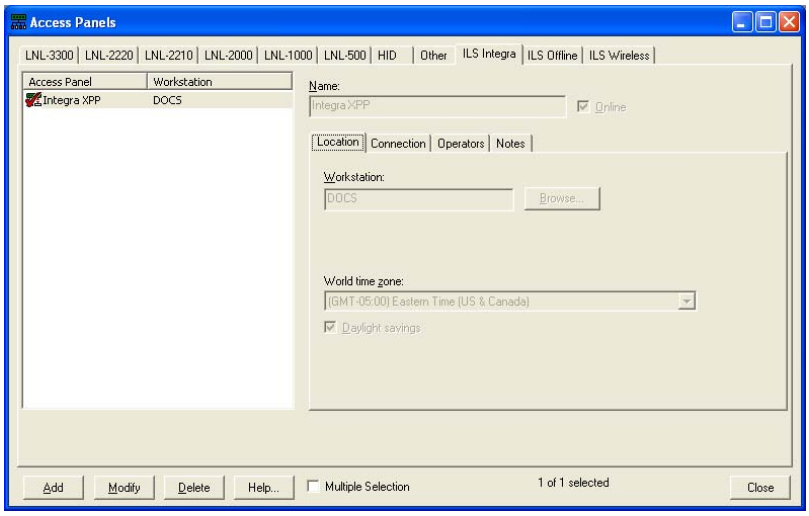
ILS Integra Form

Integra XPP devices are treated as access panels by the OnGuard software.

This form is used to:

- Assign names to Integra offline access panels in the software.
- Specify access panel setup parameters.
- Specify communication panel setup parameters, including the workstation associated with the panel.
- Add up to 16 Integra offline lock operators and their privileges.

Integra Offline Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the Integra offline panel type. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel is considered to be online. **Online** indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Select the workstation or server to which the XPP is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

World time zone

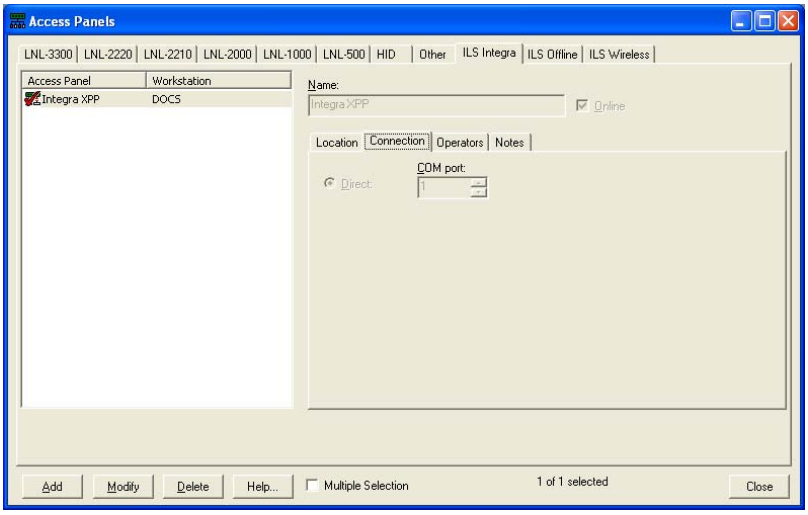
Select the world time zone for the selected access panel’s geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone’s clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Saving Time is enforced in the selected access panel's geographical location.

Integra Offline Form (Connection Sub-tab)



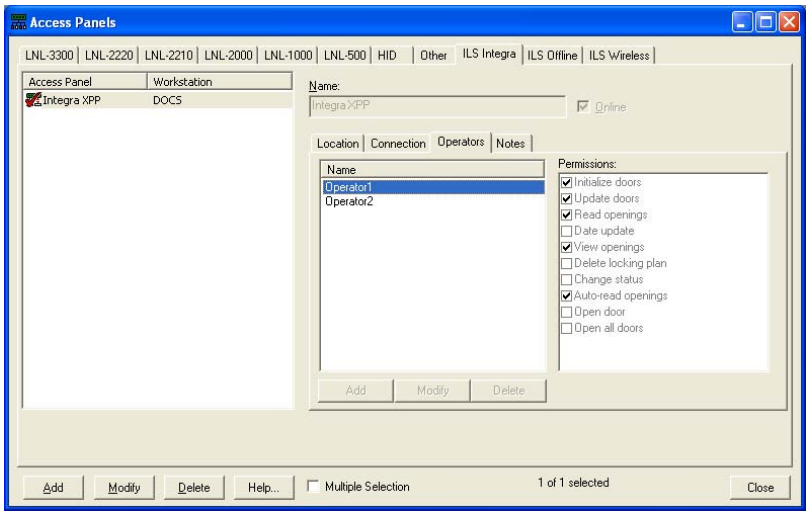
Direct

Select this radio button if for the secondary connection, communication with the access panel will be via a direct serial connection to the specified workstation. You must also specify the workstation's **COM port**.

COM port

If you selected the **Direct** radio button, specify the port that's on the serial expansion unit or the back of the workstation. To each port you can assign only one access panel. Choose a value in the range of 1 - 255.

Integra Offline Form (Operators Sub-tab)



Operators listing window

Lists the operators currently assigned to the Integra offline access panel.

Permissions

Displays the privileges specified for the Integra XPP lock operator. For permission descriptions, refer to the Add Operator Dialog on page 1478.

Add

Click this button to add an Integra XPP operator. The Add Operator dialog is displayed.

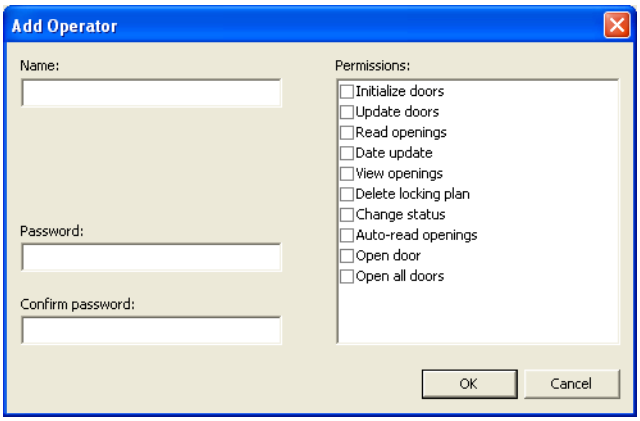
Modify

Click this button to modify the information of the selected operator. The Add Operator dialog is displayed.

Delete

Click this button to remove an operator.

Add Operator Dialog



The Add Operator dialog is displayed when you click [Add] or [Modify] to add an operator or change an operator definition.

Name

Enter a name for the user who will operate the Integra XPP portable programmer. It is a good idea to choose a name that is meaningful to the user, such as the person's initials. Maximum **Name** length is 15 characters.

Password

Enter a password that will be used to access the XPP portable programmer. Maximum **Password** length is 10 characters.

Confirm password

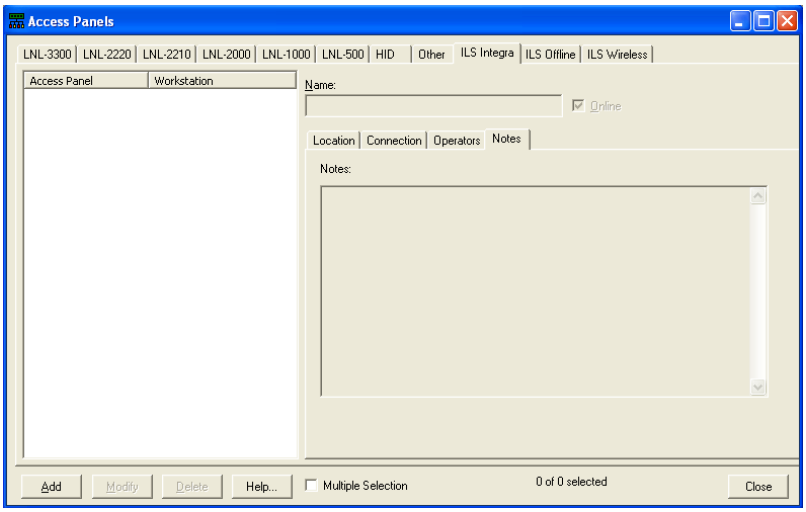
Confirm the password that you entered in the **Password** field.

Permissions

Select the privileges for the Integra XPP operator. A check box is provided for each of the operations available on the portable programmer. Choices include:

- Initialize doors - Allows the XPP operator to program a lock when it is first installed, the lock is reset, or there are system-wide changes.
- Update doors - Allows the XPP operator to update the lock with the data downloaded to the XPP from OnGuard.
- Read openings - Allows the XPP operator to retrieve lock audit data at the lock.
- Date update - Allows the XPP operator to change the date and time within the XPP. This function is commonly used to change lock time for troubleshooting or to enter a time controlled mode of operation within the lock.
- View openings - Allows the XPP operator to view the lock audit data on the XPP display. This does not affect the ability to view the lock audit data when it has been retrieved from the XPP by the computer.
- Delete locking plan - Allows the XPP operator to delete the locking plan off of the XPP. This ensures that the XPP must be reloaded to allow updates to any lock data.
- Change status - Allows the operator to change the operation mode of the lock. This function is most commonly used following initialization and testing to place the lock into the desired operating mode immediately rather than waiting for automatic scheduled timezone changes.
- Auto-read openings - Allows the XPP operator to automatically retrieve the events from the lock. If you select this option, the XPP will automatically read openings during its Update function. If this option is not selected, you may still read openings from the locks by selecting Read Openings on the XPP main menu.
- Open door - Allows the XPP operator to unlock a lock if that door’s information has been loaded into the XPP. This will even open a lock if the batteries no longer have power.
- Open all doors - Allows the XPP operator to unlock any door on the site, even if the batteries no longer have power.

Integra Offline Form (Notes Sub-tab)



Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in Monitor Devices chapter in the Alarm Monitoring User Guide.

Configure an ILS Integra Lock System

Configuring an Integra system in OnGuard requires the use of the Integra XPP portable programmer to transfer data from OnGuard to the Integra offline locks and vise versa as well as retrieve events (audits) from the locks.

To configure an Integra system in OnGuard you must first add an offline controller and define the locks by completing the following steps:

1. Add an ILS Integra Panel on page 1481.
2. Add an Integra XPP Lock Operator on page 1481.
3. Add an Integra Lock on page 1482.
4. Configure ILS System Options on page 1485.
5. Configure ILS Custom Encoding on page 1487.
6. Configure ILS Badge Types on page 1487.
7. Configure Blocking Cards for Integra Locks on page 1488.
8. Add an ILS Integra Timezone on page 1489.
9. Select Modes of Operation for Integra Locks during a Timezone on page 1490.
10. Configure the ILS Cardholder Authorization Assignments on page 1491.

ILS Integra Lock Processing

After your system is up and running…

You will also need to download the relevant configuration data stored in the OnGuard database to the ILS Integra hardware. For more information, refer to Download Integra Locks from System

Administration on page 1483. To view Integra lock events in Alarm Monitoring, use the XPP to read the events at the lock and then upload the lock data to a workstation running OnGuard. For more information, refer to Upload Integra Lock Events Using the XPP on page 1484.

ILS Integra Lock Panel Overview

The Integra offline lock panel actually refers to an XPP portable programmer. The fields configured here deal directly with the XPP portable programmer. For example, the password defined here is then entered into the XPP portable programmer when it is in use.

When Integra offline hardware requires a download, a red downwards arrow is displayed over the panel/lock device in the system tree. For more information, refer to Download Panels and Locks Overview on page 1502.

Add an ILS Integra Panel

In System Administration, complete the following steps:

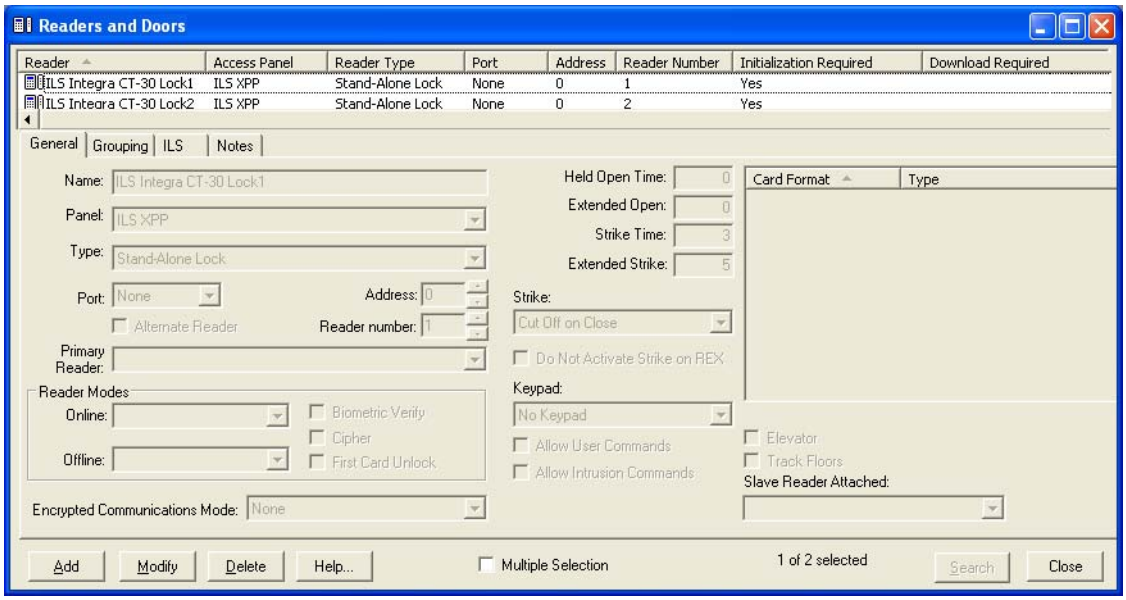
1. Select ***Access Panels*** from the ***Access Control*** menu, then select the Integra Offline tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the offline lock panel.
4. Configure the communication parameters on the Location and Connection sub-tabs. To review descriptions of these fields see the Integra Offline Form (Location Sub-tab) on page 1476 and the Integra Offline Form (Connection Sub-tab) on page 1477.
5. Add XPP lock operators. For more information, refer to Add an Integra XPP Lock Operator on page 1481.
6. Click [OK].

Add an Integra XPP Lock Operator

In System Administration, complete the following steps:

1. Select ***Access Panels*** from the ***Access Control*** menu, and then select the Integra Offline tab.
2. Click [Add] or [Modify] to add or modify the panel.
3. On the Operator sub-tab, click either [Add]. The Add Operator dialog is displayed.
4. Configure the settings for the Integra XPP operator: **Name**, **Password**, and select the operator **Permissions**. To review descriptions of these fields, refer to Add Operator Dialog on page 1478.
5. Click [OK].
6. Click [Add] to add another operator.

Integra Offline Lock Overview



In order to add an Integra offline lock you must first add an Integra offline controller. Adding an Integra offline lock is much like adding a reader for OnGuard with the exception of not having full access to all of the options as they are not supported by ILS locks. The fields that you cannot configure will not be available. The lock is added on the Readers folder General form. ILS-specific lock options are configured on the Readers folder ILS form. For more information, refer to ILS Form on page 677.

If you are adding an Integra offline lock, the **Name**, **Panel**, **Type**, **Strike Time**, and **Extended Strike** fields will be activated. **Strike Time** and **Extended Strike** can be configured from 1 - 120 seconds. Reader numbers (lock IDs) for ILS locks are unique across an Enterprise system.

Notes: Although not available when adding a lock, reader (lock) modes of operation can be configured for the start and end of a timezone. For more information, refer to Select Modes of Operation for Integra Locks during a Timezone on page 1490.

However, if you change reader modes settings, you must download the lock information from OnGuard to the lock via the XPP. For more information, refer to Download Integra Locks from System Administration on page 1483.

Add an Integra Lock

In System Administration, complete the following steps:

1. Select ***Readers*** from the ***Access Control*** menu. The Readers folder opens.
2. On the General tab, click [Add].
3. In the **Name** field, enter a unique, descriptive name for the lock.
4. In the **Panel** field, select the access panel the lock connects to. This was the ILS Integra panel (XPP portable programmer) you added in the step: Add an ILS Integra Panel on page 1481.

Note: When you select an ILS Integra panel, “Stand-Alone Lock” is automatically selected as the lock type, and the proprietary ILS card format is automatically assigned to the lock.

5. Configure the remaining options on this form as needed.

6. On the Grouping tab, configure the reader (lock) group settings. For more information, refer to Grouping Form on page 643. When reader group settings are configured, you can filter the locks displayed in the listing window using the reader search function. For more information, refer to Search for Readers by Groups on page 644.
7. On the ILS tab, configure the options as needed. For more information, refer to ILS Form on page 677.
8. Click [OK].

Download Integra Locks from System Administration

Note: Integra offline lock operators must have the **Initialize doors** and **Update doors** permissions enabled in OnGuard in order perform these operations at the door using the XPP application.

Prerequisites:

- The Integra XPP portable programmer is connected to the vacant COM port at a workstation where OnGuard and Communication Server are running.
- Unless you are familiar with the download process, first read the section Download Panels and Locks Overview on page 1502.

In System Administration, complete the following steps:

1. From the ***Access Control*** menu, select ***Readers***.
   a. In the Readers listing window, sort the locks by the Initialization Required or Download Required column, and then select the locks accordingly.
   b. Select on one or more Integra locks, right-click on them, and then select **Download** to download the lock information to the XPP connected to the workstation.
2. (Optional) From the ***Access Control*** menu, select ***Access Panels***.
   a. Click on the Integra Offline tab.
   b. In the panel listing window, right-click on the Integra panel, select **Download** to download the information from the panel, operators, and locks to the XPP connected to the workstation.
3. (Optional) Open the system tree.
   a. From the ***View*** menu, select ***System Tree***, and then select an existing window or open a new one. Expand the Hardware node, and then the Integra offline panel to show the Integra locks assigned to it.
   b. Right-click on the Integra panel, and then select **Download** to download the lock information to the XPP connected to the workstation.

Note: Downloading from the Integra offline panel will download data from the panel, operators, and all locks assigned to that panel. This is done if there is a system-wide change such as the addition of new cardholders. However, if the only the settings for one lock have changed, right-click on the lock, and then select **Download** to download the data from that lock, exclusively.

4. Disconnect the XPP from the workstation.
5. Connect the XPP to the Integra lock, and then open the XPP menu (no password is required):
   a. (Optional) If this is the first time the lock is updated, the lock was reset, or there were system-wide changes, select **Initialize Lock**. Choose the lock, and then press <Enter> to initialize the lock. For more information, refer to Download System Settings on page 1486.

b. If the lock was previously initialized, select **Update Lock**, and then click [Enter]. Choose the lock, and then press <Enter> to transfer the data from the XPP to the lock.

6. Disconnect the XPP from the lock.

View Integra Offline Lock Events

In order to view Integra lock events in Alarm Monitoring, the lock operator must use the XPP to read the events at the lock. For more information, refer to Upload Integra Lock Events Using the XPP on page 1484.

When the XPP is connected to a workstation where Alarm Monitoring is running, the lock events will be displayed automatically.

Note: The proper permissions must be configured for the XPP operator to be able to retrieve the events at the lock. For more information, refer to Add an Integra XPP Lock Operator on page 1481.

Before using the XPP at the lock, the system information must be downloaded from OnGuard to the XPP in order to update the lock. For more information, refer to Download Integra Locks from System Administration on page 1483.

Upload Integra Lock Events Using the XPP

Prerequisites: The Integra XPP portable programmer is connected to the vacant COM port at a workstation where OnGuard and Communication Server are running.

From System Administration, complete the following steps:

1. From the ***Access Control*** menu, select ***Access Panels***.
2. On the ILS Integra tab, select the Operators sub-tab.
3. Ensure at least one of the following read permissions is selected for the lock operator:
   a. **Read openings** - Select this permission in order to store events at the lock in the XPP.
   b. **Auto-read openings** - If your system has a limited number of locks, select this read permission to automatically retrieve events at the lock without entering a command. For large systems, you may want to deselect **Auto-read opening** to avoid uploading too much detail.

Note: As the lock operator, any operations you perform at the lock with the XPP require that the corresponding operator permissions are enabled in OnGuard such as **Initialize doors**, **Update doors**, or **View openings**.

4. Download the lock information. For more information, refer to Download Integra Locks from System Administration on page 1483.

Note: Downloading from the ILS Integra panel will download the data from all locks assigned to it. This is done if there is a system change such as the addition of new cardholders. However, if the only the settings for one lock have changed, select the lock icon to download the data from that lock exclusively.

5. Disconnect the Integra XPP from the workstation.
6. Connect the XPP to the Integra lock, and then open the Integra XPP menu (no password is required):
   a. (Optional) If this is the first time the lock is updated, the lock was reset, or system-wide changes were made, select **Initialize Lock**. Choose the lock, and then press <Enter> to initialize the lock. For more information, refer to Download System Settings on page 1486.

b. If the lock was previously initialized, select **Update Lock**, and then click [Enter]. Choose the lock, and then press <Enter> to transfer the data from the XPP to the lock.

c. Select **Read Openings**, and then press <Enter> to transfer the lock information to the XPP.

Note: If the **Auto-read openings** permission is enabled for the operator, Read Openings does not need to be performed because it will be done automatically.

d. Select **Show Openings**, and then press <Enter> to display the events on the XPP, and then verify that the information is valid.

7. Disconnect the XPP from the lock, and then connect it to the workstation.
8. Log into Alarm Monitoring. The lock events will be automatically displayed in the Main Alarm Monitor window.

System Options Folder - ILS Form Overview

After the ILS panel and reader (lock) have been added and configured, you must configure the ILS system options.

Use the ILS form to configure data elements that affect the programming of all ILS controllers and locks that exist in the system.

IMPORTANT: When you modify certain system settings, you must download this information to the Mobile Configurator to update or initialize the lock. For more information, refer to Download System Settings on page 1486.

Configure ILS System Options

In System Administration, complete the following steps:

1. Select ***System Options*** from the ***Administration*** menu, and then select the ILS tab. For more information about the settings configured in this procedure, refer to the ILS Form on page 419.
2. Click [Modify].
3. In the **System code** field enter the system code. This is simply a unique identifier much like a name.
4. In the **Codes look ahead** field, enter the number of codes you want to apply to all of the readers (locks) within the system.
5. Select the **Lock or card date precedence**.
6. Specify the format to **Store badge activate/deactivate dates**. Choices include:
   - None
   - Date only
   - Date and time
7. In the **Number of general authorizations** field, enter the number of authorizations that will be available for assignment.
8. (Optional) Double-click on any default Authorization item in the listing window, and then type a unique name if required.
9. To enable the Alternative Fire Code (AFC) functions on a door-by-door basis, select the **Manage Alternative Fire Code (AFC)** check box.
   a. To allow a relocking timer to be set to relock doors after they are unlocked, select the **Manage relock timer** check box.
   b. To allow individual locks to be locked automatically when the deadbolt is projected, select the Relock with deadbolt mode check box.

10. Click [OK].

Download System Settings

When you modify system-wide settings, you will need to perform either the initialization or update procedure at the lock depending on which settings are modified and the type of ILS lock.

Initialize the lock if the following settings are modified:

System Settings	ILS Offline and Wireless Locks	ILS Integra Locks
System code	X	X
Store badge activate/deactivate dates	X	
Maximum badge number length (Badge ID length) Configure this option in System Options > Hardware Settings (non-segmented systems) or the Segments > Segments > Hardware Settings sub-tab (segmented systems).	X	X

Update the lock if the following settings are modified:

System Settings	ILS Offline and Wireless Locks	ILS Integra Locks
Codes look ahead		X
AFC options	X	X
Lock or card date precedence	X	
Number of general authorizations or authorization names	X	X

Note: Locks that require initialization or updates after the ILS system options are changed are flagged for “Initialization Required” or “Download Required” in the readers listing window. You can sort the locks for downloading using the flagged columns. For more information, refer to Download Panels and Locks Overview on page 1502.

ILS Custom Encoding Overview

After the ILS system options have been configured, and if you are using a magnetic card format, you must configure the custom encoding of the magnetic card format. Doing this causes the ILS lock data to be encoded on track 3 of a magnetic card. For more information, refer to Custom Encoding Form on page 291.

For ILS Custom Encoding ensure the cardholder you are encoding the badge for has a badge PIN, badge ID, badge issue code, and proper activation and deactivation dates. For more information, refer to Badge Form on page 109. \

Required Printers/Encoders

Use one of the following printer/encoders to print encoded cards:

- Fargo HDP5000 printer equipped with an ISO magnetic encoder, using driver version 2.0.0.5 or later
- Rio/Tango 2e card printer equipped with an ISO magnetic encoder, using driver version 1.3.4.0 or later
- MSR206 magnetic stripe encoder is used to encode the ILS card data

Configure ILS Custom Encoding

In System Administration, complete the following steps:

1. From the ***Administration*** menu, select ***Card Formats***. The Card Formats folder opens. For more information, refer to Custom Encoding Procedures on page 299.
2. In the listing window, select any magnetic card format.
3. Click [Modify].
4. Click the Custom Encoding sub-tab.
5. Select the **Track 3** radio button.
6. In the Edit Custom Field section, select the **ILS Magnetic Data (Track 3 Only)** radio button.
7. In the Edit Custom Field section, click [Add]. **Track 3** populates to read: "<<ILS Magnetic Data>>." Optionally, if you are configuring an existing card format and you want to preserve existing data located on track 1 and 2 then:
   a. Select the **Track 1** radio button and click [Delete].
   b. Select the **Track 2** radio button and click [Delete].
   c. Select the Card Format sub-tab.
   d. Change the **Total Characters on Track 2** field to "0".
   e. Change all of the **Access Control Fields on Track 2** fields to "0".
8. Click [OK].

ILS Badge Types Overview

Optionally, you can configure the ILS badge types so they allow you to encode authorizations to badge types that get assigned to cardholders.

Configure ILS Badge Types

In System Administration, complete the following steps:

1. From the ***Administration*** menu, select ***Badge Type***, and then select the ILS tab.
2. In the listing window, select the badge type you want to configure.
3. Select the authorization you want to assign as the default to a cardholder badge of this ILS badge type.
4. Select the options that you want to enable in the Optional encoding fields section of the window. For more information, refer to ILS Form on page 332.
5. Click [OK].

Integra Blocking Cards Overview

IMPORTANT: Blocking cards for Integra CT30 locks are not to be confused with blocking cards for ILS offline/wireless locks which have a different configuration. For information about configuring a blocking card for ILS wireless locks, refer to Configure Special Purpose Cards for ILS Offline/Wireless Locks on page 1511.

Integra blocking cards are used to deny access through doors, even to users with valid cards who would normally be able to open the locks on those doors. A blocking card allows personnel with the proper authority to limit traffic in certain areas, such as those under police investigation. A single blocking card can be used to block access to any number of locks.

In OnGuard, the system administrator creates a cardholder badge that is used as the blocking card.

IMPORTANT: This card (badge) must be assigned to every lock to which it will be downloaded. To assign this card to the locks, an access level must be added that contains the locks, and then that access level is assigned to the card on the Cardholders folder > Access Level form. For more information, refer to Assign Access Levels to a Badge on page 118.

Note: If a cardholder is assigned to a badge configured to override blocking, that badge will unlock a door that is blocked by a blocking card. For more information, refer to Add a Badge Template on page 199.

Configure Blocking Cards for Integra Locks

Prerequisite: Ensure manual Badge ID entry is enabled.

(From the ***Administration*** menu, select either ***Cardholder Options*** or ***Badge Types***. On the Badge ID Allocation form, select the ID Allocation tab, and then select “Manual Entry” from the **Generate Badge ID** drop-down.)

From System Administration, complete the following steps:

1. From the ***Administration*** menu, select ***Cardholders***.
2. Click [Add].
3. On the Badge tab:
   a. The **Last name** field is required so you must enter something here (for example, “Blocking card”).
   b. Type “65001” in the **Badge ID** field.
   c. From the **Badge type** drop-down, select the ILS badge type you configured in Configure ILS Badge Types on page 1487.
   d. Click [OK].
4. On the Access Levels tab:
   a. Click [Modify].
   b. Assign an access level to the badge. This access level should contain the readers (locks) you want to block with the blocking card. For more information, refer to Assign Access Levels to a Badge on page 118.

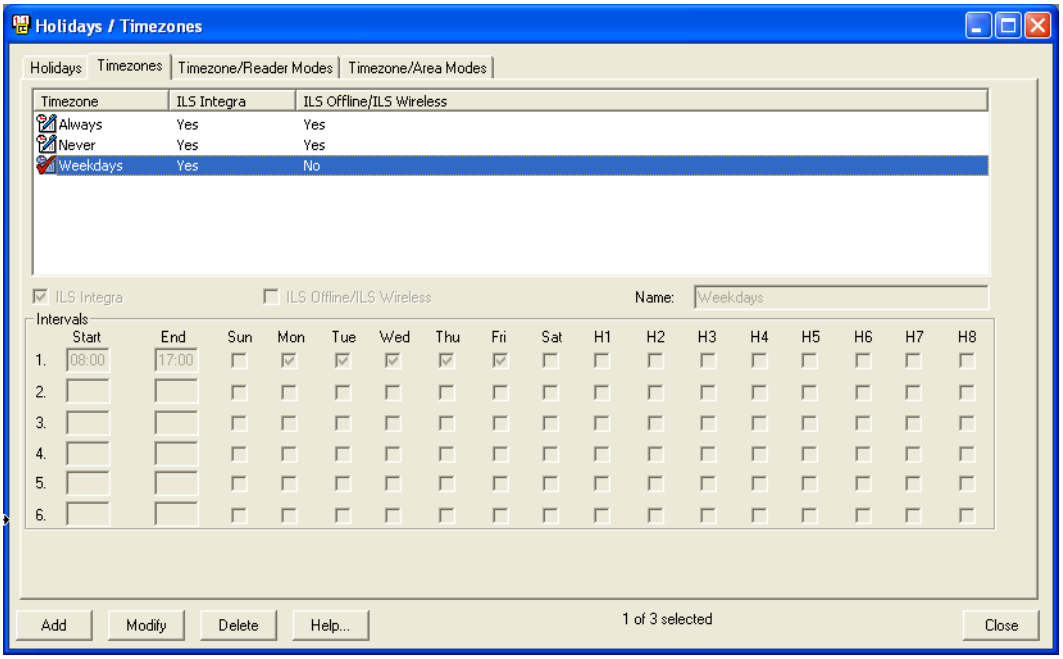
   Note: ILS readers (locks) do not support assigning an access level to the card if that access level contains a lock that is in an access level already assigned to the card.

   c. Click [OK].

5. Click [Print] to encode the blocking card using the printer/encoders listed in Required Printers/ Encoders on page 1487.
6. Download the blocking card to the XPP programmer to update the locks in your system.

Note: If you need to create a new set of blocking cards, be sure to increment the **Issue code** by 1. When the **Issue code** is incremented, and new blocking cards are printed, this will make the previous set of blocking cards invalid.

ILS Integra Timezones Overview



Optionally, you can use the Timezones form to create timezones which will be downloaded to Integra CT30 locks. Each ILS Integra timezone consists of up to five (5) time range/day intervals. Up to a maximum of 32 Integra timezones are allowed including the two (2) system time intervals, Always and Never.

Note: An ILS Integra timezone must be associated with an ILS Integra reader (lock) in order to assign it to Timezone/Reader Modes or Access Level configurations.

Add an ILS Integra Timezone

In System Administration, complete the following steps:

1. Select ***Timezones*** from the ***Access Control*** menu, and then select the Timezones tab.
2. Click [Add].
3. Select the **ILS Integra** check box to indicate this timezone is to be downloaded to Integra offline locks.
4. Type a name for the timezone in the **Name** field.
5. Define each time interval in this timezone, including the start and end times, the specific days of the week, and the holiday types you want. Enter **Start** and **End** times, and then select the check boxes you want the time range to apply to.
6. Click [OK].

ILS Integra Timezones/Reader Modes Overview

Optionally, you can use the Timezones/Reader Modes form to configure up to 10 scheduled mode changes per lock. For more information, refer to Timezone/Reader Modes Form on page 711.

Examples of possible ILS Integra configurations:

- 2 timezones containing 5 intervals each
- 5 timezones containing 2 intervals each
- 10 timezones containing 1 interval each

Select Modes of Operation for Integra Locks during a Timezone

In System Administration, complete the following steps:

1. Select ***Timeszones*** from the ***Access Control*** menu.
2. On the Timezone/s tab listing window, select the reader (lock) you want to control the operation of during a particular timezone. This was the Integra lock you added in the step: Add an Integra Lock on page 1482.
3. Click [Modify].
4. Choose the **Timezone** you want to configure for the selected reader (lock). This was the Integra timezone you added in the step: Add an ILS Integra Timezone on page 1489.
5. In the Start section, from the drop-down, select the mode you want this lock to be placed in at the *beginning* of the selected timezone:
   - Card and Pin
   - Card and Pin Unlocked
   - Card Only
   - Cipher or Card
   - Unlocked
   - First Card Unlock
6. In the End section, from the drop-down, select the mode you want this lock to be placed in at the *end* of the selected timezone.
7. Click [Assign]. The following actions happen immediately:
   - The change is saved to the database.
   - The assignment window is updated.
   - The settings are not downloaded immediately. Instead, the lock's offline panel is flagged for a download to the XPP in the system hardware tree or the Readers and Doors folder.

   Functionally, at the start of the selected timezone, the selected reader (lock) will begin to function in the selected **Start mode**. The lock remains in that mode until the end of the timezone at which time the lock will be placed in the selected **End mode**.
8. Repeat steps 4 - 7 for each additional timezone you want to configure for this lock.
9. Click [OK] to return to view mode. The listing window will be updated to reflect your changes.
10. Repeat this procedure if you want to set up the operating modes of other locks.

Note: You will need to download the lock information to the lock via the XPP. For more information, refer to Download Integra Locks from System Administration on page 1483.

ILS Cardholder Authorization Assignments Overview

Optionally, you can configure ILS cardholder authorization assignments so that you can customize a cardholder's accessibility to locks and limit their access to areas without needing to update the locks.

Configure the ILS Cardholder Authorization Assignments

In System Administration, complete the following steps:

1. Select ***Cardholders*** from the ***Administration*** menu, then select the ILS Authorizations tab.
2. Locate the cardholder that you want to assign ILS authorization to.
3. Click [Modify].
4. In the authorization listing window, select the authorizations that you want the cardholder to have. For more information, refer to ILS Authorization Form on page 136.
5. Click [OK]. The cardholder now has access to the authorization levels you have selected.

ILS Badge Templates Overview

Optionally, you can configure ILS badge templates. Badge Templates can be downloaded to an ILS lock and assigned to an individual cardholder. Badge templates are ideally suited for dynamic environments where cardholders change frequently. Badge templates can be used to avoid numerous data downloads to the locks that are in such a dynamic environment.

For more information, refer to Chapter 7: Badge Templates Folder on page 195.

ILS Offline/Wireless Locking Systems Overview

OnGuard allows you to set up ILS offline locking systems using ILS wireless-capable locks (commonly referred to in OnGuard as readers) and ILS Offline controllers (Mobile Configurators) that are treated as access panels by OnGuard.

In an ILS offline lock configuration, OnGuard acts as a front end to the data transferred between OnGuard and the ILS offline locks via the Mobile Configurator. For more information, refer to Configure an ILS Offline Locking System on page 1497.

Note: ILS locks assigned to an ILS Offline controller (Mobile Configurator) can be re-assigned to a different ILS Offline controller or to an ILS Wireless controller (Wireless Gateway) within the same segment. For more information, refer to Modify ILS Offline Panel Assignment on page 1501.

OnGuard also allows you to set up ILS wireless locking systems using ILS wireless locks (commonly referred to in OnGuard as readers) and ILS Wireless Gateways that are treated as access panels by OnGuard.

In an ILS wireless configuration, the ILS Wireless controller, acting as an ILS Wireless Gateway, provides a communication link between OnGuard and the ILS wireless locks, allowing for an exchange of data between the two. For more information, refer to Configure an ILS Wireless Locking System on page 1518.

Up to 32 readers (locks) can be assigned to a Wireless Gateway device.

Note: ILS locks assigned to an ILS Wireless controller (Wireless Gateway) can be re-assigned to a different Wireless Gateway within the same segment. For more information, refer to Modify ILS Wireless Panel Assignment on page 1522.

IMPORTANT: ILS readers (locks) do not support assigning an access level to a cardholder (badge) if that access level contains a lock that is in an access level already assigned to the cardholder (badge).

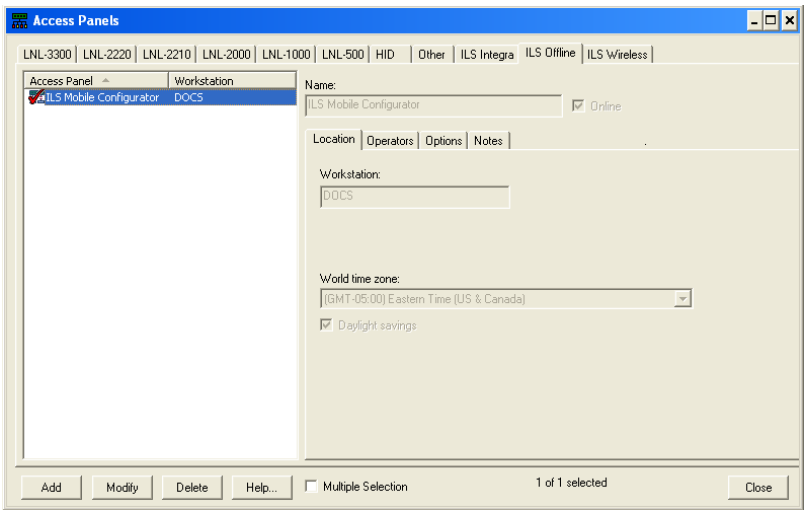
ILS Offline Form

The ILS offline controllers (Mobile Configurators) are treated the same as access panels by OnGuard.

This form is used to:

- Assign names to ILS offline controllers in the software.
- Specify ILS offline controller setup parameters.
- Add up to 100 ILS offline lock operators and their privileges.

ILS Offline Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the ILS offline panel type. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel is considered to be online. **Online** indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Displays the workstation to which the Mobile Configurator is connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. When you connect a Mobile Configurator to the workstation, the system enters the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

It is not necessary to specify a workstation when configuring an ILS offline controller. The data is downloaded to the Mobile Configurator by connecting it to a workstation where System Administration is running. In addition, Communication Server must be installed and running on the workstation. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505. If you are using the Mobile Configurator with OnGuard on a Windows XP, Windows 2003, or Windows 2008 system, Communication Server must be run as an application.

World time zone

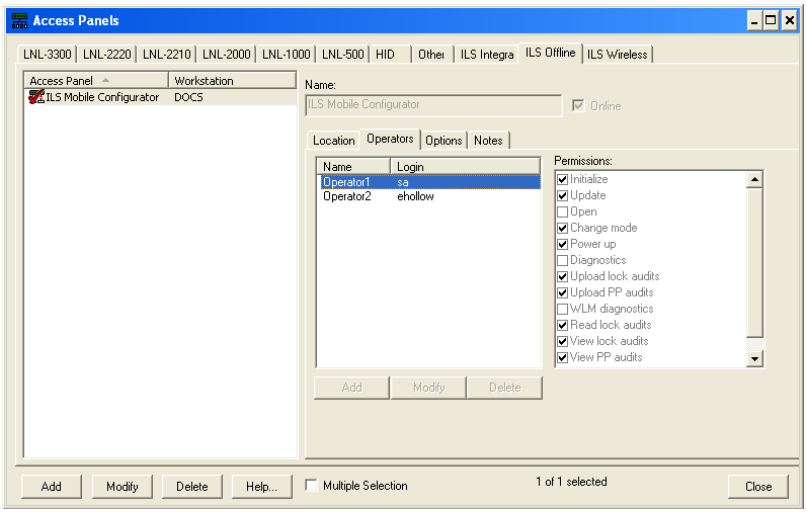
Select the world time zone for the selected access panel's geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

Daylight savings

Select this check box if Daylight Saving Time is enforced in the selected access panel's geographical location.

ILS Offline (Operators Sub-tab)



Operators listing window

Lists the operators currently assigned to the ILS offline access panel.

Permissions

Displays the privileges specified for the Mobile Configurator operator. Descriptions of each permission are provided in Add Operator Dialog on page 1478.

Add

Click this button to add a Mobile Configurator operator. The Add Operator dialog is displayed.

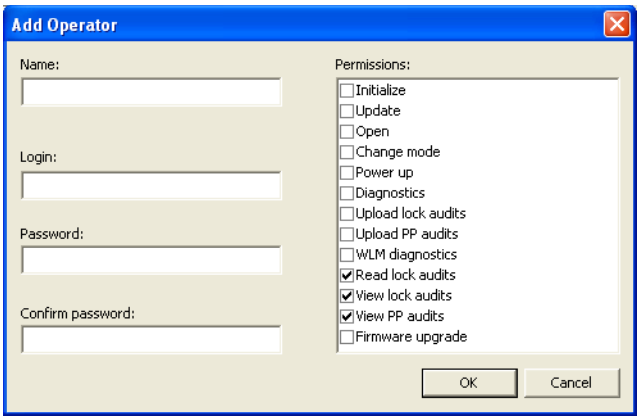
Modify

Click this button to modify the information of the selected operator. The Add Operator dialog is displayed.

Delete

Click this button to remove an operator.

Add Operator Dialog



The Add Operator dialog is displayed when you click [Add] or [Modify] to add an operator or change an operator definition. You can add up to 100 operators to an ILS offline panel (Mobile Configurator).

Name

Enter a name for the user who will operate the ILS Mobile Configurator. It is a good idea to choose a name that is meaningful to the user, such as the person's initials. Maximum Name length is 15 characters. When events are uploaded from the Mobile Configurator to Alarm Monitoring, events that have an operator associated with them will be displayed with the operator name in the Operator column. For more information, refer to the Alarm Monitoring User Guide.

Login

Enter a login name for the user. Maximum Login is 10 characters.

Password

Enter a password that will be used to access the ILS offline Mobile Configurator. Maximum Password length is 10 characters. Password must contain at least one (1) number.

Confirm password

Confirm the password that you entered in the **Password** field.

Permissions

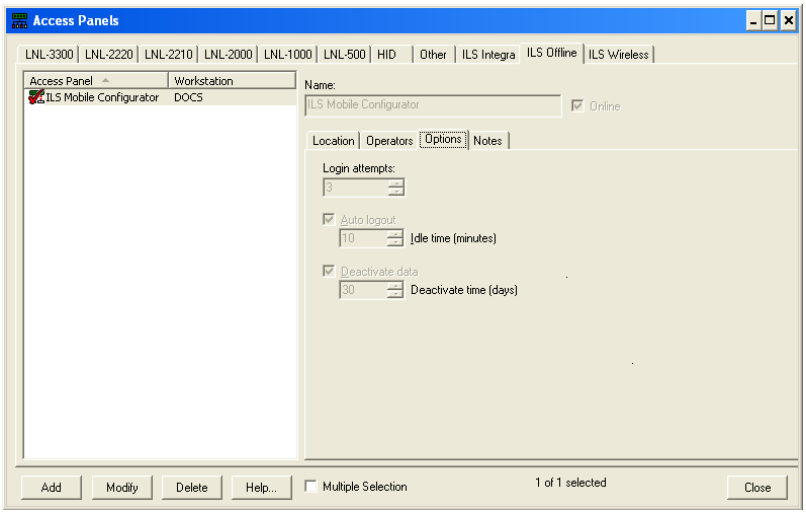
Select the privileges for the operator of the Mobile Configurator. Choices include the following (**Read lock audits**, **View lock audits**, and **View PP audits** are the default selections):

- **Initialize** - Allows the operator to program a lock when it is first installed, the lock is reset, or when system-wide changes are made.
- **Update** - Allows the operator to update the lock with the data downloaded from OnGuard to the Mobile Configurator.
- **Open** - Allows the operator to unlock a lock if that door's information has been loaded into the Mobile Configurator. This will even open a lock if the batteries no longer have power.
- **Change mode** - Allows the operator to change the reader mode of the lock to Card Only, Facility Code Only, Unlocked, First Card Unlock, Blocked, Secured, or Unsecured. This function is most commonly used following initialization and testing to place the lock into the desired operating mode immediately rather than waiting for scheduled timezone changes. In addition, this permission allows the operator to check the current operational mode of the lock.
- **Power up** - Allows the operator to power up the lock from outside in case the battery power is low or the battery has no power.
- **Diagnostics** - Allows the operator to perform diagnostics on the lock including the following options:
  - Switch test for the Handle, Card, Privacy, Mechanical Key Override, Clear, Latch Monitor, and Door Sensor switches.
  - LED and buzzer test. During this test, the lock LED alternates between Red and Green for five (5) seconds, followed by a high and low pitched beep sound.
  - Lock battery level test. When the battery level is low (18 percent or less), a warning message is displayed on the Mobile Configurator.
  - View the lock information such as lock date and time, firmware version, hardware version, manufacturing date, and the serial number of the circuit board.
- **Upload lock audits** - Allows the operator to upload the lock events from the Mobile Configurator to Alarm Monitoring.
- **Upload PP audits** - Allows the operator to upload events performed by the Mobile Configurator (Portable Programmer) on the lock or on the Mobile Configurator itself such as operator login, synchronizing the Mobile Configurator date and time, clearing locking plans in the Mobile Configurator, etc.
- **WLM diagnostics** - Allows the operator to perform Wireless Lock Module (WLM) tests.
- **Read lock audits** - Allows the operator to get the current audit trails of the lock and store them in the Mobile Configurator. After all of the data is transferred to the Mobile Configurator, the Real-Time Clock (RTC) of the lock is updated.
- **View lock audits** - Allows the operator to view the lock audits of a specified lock on the Mobile Configurator.
- **View PP audits** - Allows the operator to view the Mobile Configurator (Portable Programmer) events such as logging in and the Mobile Configurator operations on the lock such as initializing the lock, updating the lock, reading lock audits, running tests, etc.

Note: For the audit permissions, the audit information includes operator name, date and time of the audit, operations/events, and the record number (lock ID).

- **Firmware upgrade** - Allows the operator to upgrade the firmware on the lock.

ILS Offline Form (Options Sub-tab)



Login attempts

Specifies the maximum number of invalid login attempts allowed for the Mobile Configurator application. Maximum **Login attempts** is 20.

Auto logout

Select this check box to automatically log out of the Mobile Configuration application after a specified period of idle time.

Idle time (minutes)

Specifies the length of idle time after which the Mobile Configuration application is automatically logged off. Maximum **Idle time** is 120 minutes.

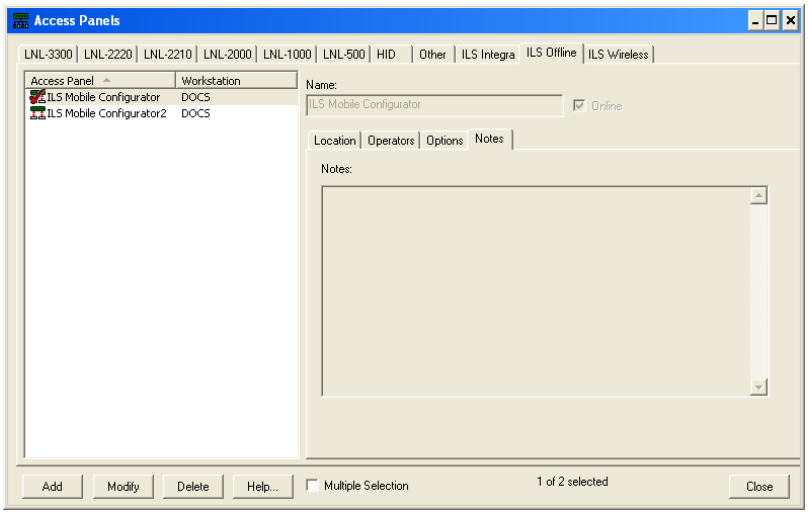
Deactivate data

Allows automatic deletion of the data downloaded to the Mobile Configurator after the specified **Deactivate time**.

Deactivate time (days)

Specify the number of days after which the data downloaded to the Mobile Configurator is automatically deleted provided the lock operator has not used the system for the time specified. Maximum **Deactivate time** is 120 days.

ILS Offline Form (Notes Sub-tab)



Notes

Enter information about the panel. This field is limited to less than 2000 characters.

Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Monitor Devices chapter in Alarm Monitoring.

Configure an ILS Offline Locking System

Configuring an ILS offline locking system in OnGuard requires the use of the ILS offline controller (Mobile Configurator) to transfer data from OnGuard to the ILS locks and vice versa as well as retrieve events (audits) from the locks. For information on the Mobile Configurator, refer to the ILS Lock Operation User Guide.

To begin configuring the ILS offline locking system in OnGuard you must first add a Mobile Configurator and define the doors/locks by completing the following steps:

1. Add an ILS Offline Access Panel on page 1498.
2. Add a Mobile Configurator Lock Operator on page 1498.
3. Add an ILS Offline Lock on page 1500.
4. Modify ILS Offline Panel Assignment on page 1501.
5. Configure ILS System Options on page 1485.
6. Configure ILS Custom Encoding on page 1487.
7. Configure ILS iCLASS Printing and Encoding on page 1513.
8. Configure ILS Badge Types on page 1510.
9. Configure Special Purpose Cards for ILS Offline/Wireless Locks on page 1511.
10. Add an ILS Offline/ILS Wireless Timezone on page 1508.
11. Select Modes of Operation for ILS Locks during a Timezone on page 1509.
12. Configure the ILS Cardholder Authorization Assignments on page 1491.

ILS Offline Lock Processing

After your system is up and running...

You will also need to download the relevant configuration data stored in the OnGuard database to the ILS offline locks as needed. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505. To view ILS offline lock events in Alarm Monitoring, the lock information is uploaded to the Mobile Configurator which is then connected to a workstation where OnGuard is running. For more information, refer to Upload ILS Offline Lock Events Using the Mobile Configurator on page 1507.

ILS Offline Lock Panel Overview

The ILS offline lock panel actually refers to a ILS Mobile Configurator. The fields configured here deal directly with the Mobile Configurator. For example, the password defined here is then entered into the Mobile Configurator when it is in use.

When ILS offline hardware requires a download, a red downwards arrow is displayed over the panel/lock device in the system tree. For more information, refer to Download Panels and Locks Overview on page 1502.

Add an ILS Offline Access Panel

In System Administration, complete the following steps:

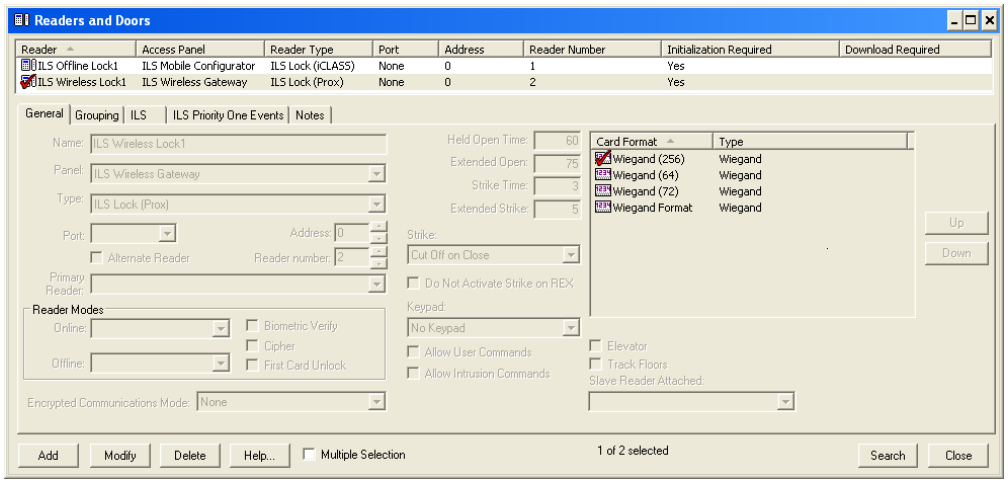
1. Select ***Access Panels*** from the ***Access Control*** menu, and then select the ILS Offline tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the ILS offline lock panel.
4. On the Location sub-tab, configure the **World time zone** and **Daylight savings** settings. To review the specifics regarding these fields, refer to the ILS Offline Form (Location Sub-tab) on page 1492.
5. On the Options sub-tab, configure the **Login attempts**, **Auto logout**, and **Deactivate time**. To review the specifics regarding these fields, refer to the \.
6. Add the Mobile Configurator lock operators. For more information, refer to Add a Mobile Configurator Lock Operator on page 1498.
7. Click [OK].

Add a Mobile Configurator Lock Operator

In System Administration, complete the following steps:

1. Select ***Access Panels*** from the ***Access Control*** menu, and then select the ILS Offline tab.
2. Click [Add] or [Modify].
3. On the Operator sub-tab, click [Add]. The Add Operator dialog is displayed.
4. Configure the ILS offline operator settings: **Name**, **Login**, **Password**, and select the operator **Permissions**. To review the specifics regarding these fields, refer to the Add Operator Dialog on page 1478.
5. Click [OK].
6. Click [Add] to add more operators.

ILS Offline Lock Overview



To add an ILS offline lock you must first add an ILS offline controller. Adding an ILS offline lock is much like adding a reader for OnGuard with the exception of not having full access to all of the options as they are not supported by ILS locks. The fields you cannot configure will not be available.

When you add ILS offline locks, the **Name**, **Panel**, **Type**, **Held Open Time**, **Extended Open**, **Strike Time**, and **Extended Strike** fields will be activated. **Extended Strike** and **Extended Open** are typically used with the ADA feature. However, if **Lock when lever is released** is enabled for the lock, the lock will re-engage after the cardholder turns the lever. This and the other ILS-specific lock options can be configured on the ILS Form on page 677.

Card formats for ILS locks are selected for specific lock types, and can be prioritized and sorted. For more information, refer to Lock Card Formats on page 1499.

Note: Reader numbers (lock IDs) for ILS locks are unique across an Enterprise system.

Note: Although not available when adding a lock, reader (lock) modes of operation can be configured for the start and end of a timezone. For more information, refer to Select Modes of Operation for ILS Locks during a Timezone on page 1509.

IMPORTANT: When you change the lock settings, this information must be downloaded from OnGuard to the lock using the Mobile Configurator. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505.

Lock Card Formats

Identify the format(s) expected when a card is presented to a reader. Card formats are defined in the Card Formats folder.

For iCLASS lock types, the card format list is presented with two (2) sub-tabs:

- Smart Card Formats: Select this tab to assign up to four (4) smart card formats.
- Access Control Card Formats: Select this tab to assign up to four (4) Wiegand access control card formats.

Note: You must select at least one card format from the Smart Card Formats (iCLASS) AND one from the Access Control Card Formats (Prox).

For magnetic lock types, the card format is automatically assigned to the lock. The system uses a pre-defined, ILS-proprietary magnetic card format.

Note: ILS supports Magnetic, Prox (HID, AWID, Lenel Prox) and, depending on your version of OnGuard, Smart Card (Lenel iCLASS, HID iCLASS, CSN for iCLASS, and Lenel MIFARE and CSN for MIFARE).

Prioritize Card Formats

Card formats are sorted by priority, highest (top) to lowest (bottom), followed by unassigned card formats in ascending name order. Card formats can be moved up or down by using the priority [Up] or [Down] buttons. These buttons are only available for ILS iCLASS and proximity ILS locks.

The priority level determines the order in which card formats are used by the lock to access card data. When the lock retrieves the data from the card, it will attempt to use the card format with the highest priority, and then process the data according to that format. If the card format is successfully used to retrieve the data from the card, no other card format is attempted.

Sort Card Formats

Click on the Card Format column to sort the card formats. The order for selected and prioritized items will be preserved based on their priority. In addition, the list is dynamically sorted each time the following changes are made:

- When you select a card format, it is given the next priority.
- When you select a card format with a priority, and then click [Up] to raise it in the list or [Down] to lower its priority.
- When you unassign (deselect) a card format, its priority is removed and the other card formats are re-prioritized.

Multiple Selection

During multiple selection, the card format list is disabled unless the selected readers are of the same type or are Lenel readers.

Add an ILS Offline Lock

Note: Optionally, you can configure multiple ILS offline locks using the ***Application*** > ***Wizards*** menu option in System Administration. For more information, refer to Application Menu on page 60.

In System Administration, complete the following steps:

1. Select ***Readers and Doors*** from the ***Access Control*** menu. The Readers folder is opened.
2. On the General tab, click [Add].
3. In the **Name** field, enter a unique, descriptive name for the lock.
4. In the **Panel** field, select the access panel to which you want to connect the reader. This is the ILS offline panel (Mobile Configurator) you added in the step: Add an ILS Offline Access Panel on page 1498.
5. In the **Type** field, select an ILS lock type. Choices include:
   - ILS Lock (Magnetic)
   - ILS Lock (iCLASS)
   - ILS Lock (MIFARE)

- ILS Lock (Prox)

Note: When the lock type is selected, this determines which card formats are available for assignment to the lock.

6. Select one or more card formats.

Note: ILS supports up to four (4) Wiegand card formats for iCLASS, MIFARE, and proximity type locks and, depending on your version of OnGuard, up to four (4) smart card formats for iCLASS and MIFARE locks, only.

- If you selected "ILS Lock (Magnetic)" the card format is automatically assigned.
- For iCLASS locks, you must select at least one iCLASS card format from the Smart Card Formats sub-tab AND the appropriate Wiegand card formats from the Access Control Card Formats sub-tab. Smart card formats supported by ILS iCLASS locks include Lenel (iCLASS). For more information, refer to Add a Lenel (iCLASS) Smart Card Format on page 276.
- For proximity locks, select the appropriate Wiegand card formats from the Access Control Card Formats sub-tab, only.
- (Depending on your version of OnGuard, this option may not be available.)
  For MIFARE locks, you must select at least one MIFARE card format from the Smart Card Formats sub-tab AND the appropriate Wiegand card formats from the Access Control Card Formats sub-tab. Smart card formats supported by ILS MIFARE locks include Smart Card CSN and Lenel (MIFARE). For the Smart Card CSN card format, "ISO 14443A" must be configured as the **Credential Type**. For more information, refer to Add a Smart Card CSN Card Format on page 279 and Add a Lenel (MIFARE) Smart Card Format on page 277.

7. Prioritize the card formats as required. For more information, refer to Prioritize Card Formats on page 1500.
8. Configure the remaining settings as needed.
9. On the Grouping tab, configure the reader (lock) group settings. For more information, refer to Grouping Form on page 643. When group settings are configured, you can filter the locks displayed in the listing window using the reader search function. For more information, refer to Search for Readers by Groups on page 644.
10. On the ILS tab, configure the settings as needed. For more information, refer to ILS Form on page 677.
11. Click [OK]. The lock is added and automatically flagged in the Initialization Required column.

Modify ILS Offline Panel Assignment

Locks assigned to ILS offline panels can be reassigned to a different ILS offline or to an ILS wireless panel within the same segment. For more information, refer to Modify ILS Wireless Panel Assignment on page 1522.

Prerequisites: Ensure you are in single selection mode.

Note: Locks assigned to ILS offline panels can be reassigned to a different ILS offline or wireless panel within the same segment. However, locks assigned to ILS wireless panels can only be reassigned to a different ILS wireless panel.

In System Administration, complete the following steps:

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. From the list, select the lock you are changing.

3. On the General tab, click [Modify].
4. In the **Panel** field, select the ILS offline or ILS wireless panel to which you want to reassign the lock, and then click [OK].

Modify ILS Offline Lock Type

After a lock is added, you can modify the lock's **Type** to accommodate upgrades/changes to the lock's card technology such as changing from a magnetic lock to a proximity lock or from a proximity lock to an iCLASS lock. This change also requires that you select card formats for the new lock type.

Note: Reader (lock) type has an impact on battery life. Proximity and iCLASS reader field excitation enters a low power mode when no card is present.

Download Panels and Locks Overview

ILS Integra/offline panel and lock information can be downloaded from the Readers folder, the Access Panels folder, or the system tree. For more information, refer to Download ILS Offline/ Wireless Locks from System Administration on page 1505 or Download Integra Locks from System Administration on page 1483.

ILS wireless locks are downloaded wirelessly. In addition, ILS wireless locks can be downloaded from the Alarm Monitoring system status tree. For more information, refer to Download ILS Wireless Locks in the Alarm Monitoring User Guide.

Note: Although ILS wireless locks are automatically downloaded to the Wireless Gateway, you may need to update the lock data using a Mobile Configurator if there is a communication problem or power is lost at the wireless lock. In addition, ILS wireless locks must be initialized via the Mobile Configurator.

• WARNING! • The maximum number of cardholders (badges) that can be downloaded to an ILS offline/wireless lock is limited to 50,000 bytes based on the size of the cardholder (badge) information. An alarm will be generated if the maximum amount of cardholder data is exceeded. For more information, refer to Calculate Maximum Cardholders on page 1504.

The Readers folder listing window includes two (2) columns that indicate if a download action needs to be performed for the lock (marked "Yes"). After the action is completed at the lock, and the events are received at OnGuard, the indication will be cleared. The columns include:

Initialization Required. Indicates the lock information needs to be downloaded to the Mobile Configurator or XPP (Integra), and then used to initialize the lock. All ILS locks must be initialized whenever certain system settings are changed. When a new lock is added, it is automatically marked "Initialization Required."

Note: Before initializing the lock, you must reset the lock to factory settings. For more information, refer to the ILS Lock Operation User Guide.

Download Required. Indicates the ILS Integra/offline lock information needs to be downloaded to the XPP or Mobile Configurator, and then used to update the lock. ILS wireless locks do not require this operation because they are updated wirelessly. ILS Integra/offline locks must be updated whenever certain system settings are changed.

For more information, refer to Download System Settings on page 1486.

In the system tree, ILS Integra/offline panels and readers (locks) that require a download are flagged with a red downwards arrow in the system hardware tree.

Download Required Icons

	Access panel
	Reader (lock)

If an ILS Integra/offline lock requires a download, the panel device to which that lock is assigned will be flagged for a download as well.

IMPORTANT: The download required icons for ILS Integra/offline locks are not cleared until the physical locks have been initialized or updated, and these events are communicated to OnGuard via the XPP or Mobile Configurator.

Available Download Commands

Reader (Lock)	Download Command	Download to Portable Device Command	Device
ILS Integra	X		XPP
ILS Offline	X	X	Mobile Configurator
ILS Wireless	X	X	Wireless Gateway or Mobile Configurator

Download Commands

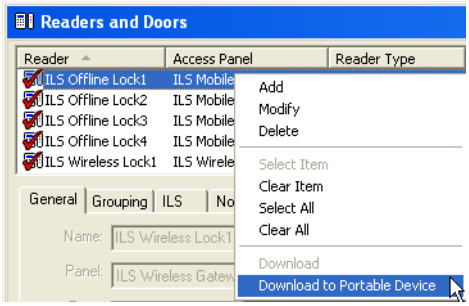
- If the locks belong to the one or more ILS wireless panels, the lock information is downloaded directly to the locks via their corresponding Wireless Gateway.
- If the locks belong to the same ILS offline panel, the lock information is downloaded to their corresponding Mobile Configurator.
- If the locks belong to the same ILS Integra panel, the lock information is downloaded to their corresponding XPP.

Note: For ILS Integra/offline locks, the lock information is downloaded with the panel and operator settings. For ILS wireless locks, the lock information is downloaded with the panel settings.

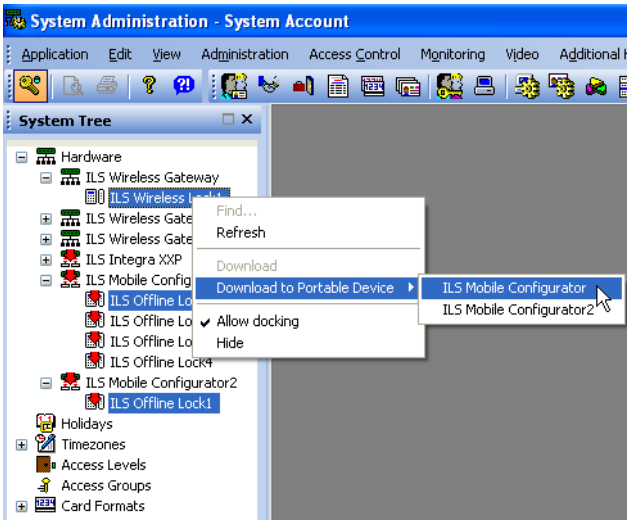
Download to Portable Device Command

IMPORTANT: In order to **Download to a Portable Device**, the locks selected for the download must be in the same segment.

- If the locks belong to the same ILS offline panel (and optionally to one or more ILS wireless panels), the lock information will be downloaded to their corresponding Mobile Configurator (panel).



- If the locks belong to several ILS offline panels (and optionally to one or more ILS wireless panels), the system will prompt you to choose which ILS offline panel to use for downloading to the Mobile Configurator.



- If the locks belong to one or more ILS wireless panels, and there is only one ILS offline panel in the segment, the lock information will be downloaded to the ILS offline panel (Mobile Configurator) in the segment.
- If the locks belong to several ILS offline panels, and there are several ILS offline panels in the segment, the system will prompt you to choose which ILS offline panel to use for downloading to the Mobile Configurator.

Calculate Maximum Cardholders

OnGuard limits the number of cardholders downloaded to the Mobile Configurator or sent via the Wireless Gateway to the capacity of the lock. ILS offline/wireless locks support up to 50,000 bytes of data. An alarm will be generated if the maximum amount of cardholder data is exceeded.

Cardholder (badge) record size is calculated as follows:

Badge ID Length (2 - 8 bytes) + 2 * Activate/Deactivate Date Format (0, 2, 5 bytes) + Issue Code (4 bytes) + Configuration Parameters (3 bytes)

The Activate/Deactivation Date Format is taken from the **Store badge activate/deactivate dates** system option:

- None (0 bytes)
- Date only (2 bytes)

- Date and time (5 bytes)

Badge IDs require 4 - 8 bytes of memory, depending on the number of digits in a badge.

- 7 - 9 digits require 4 bytes
- 10 - 12 digits require 5 bytes
- 13 - 14 digits require 6 bytes
- 15 - 16 digits require 7 bytes
- 17 - 18 digits require 8 bytes

Example: If Badge ID length is 14 (6 bytes) and the Activate/Deactivate Date Format is “Date and time” (2 * 5 bytes), add 16 bytes to 4 bytes + 3 bytes (Issue Code + Configuration Parameters) = 23 bytes per record.

50,000/23 = 2173.91 maximum cardholders

Download ILS Offline/Wireless Locks from System Administration

Prerequisites:

- The Mobile Configurator is connected to a vacant USB port at a workstation where Microsoft Active Sync, OnGuard, and Communication Server are running.

  IMPORTANT: If you are using the Mobile Configurator with OnGuard on a Windows XP, Windows 2003, or Windows 2008 system, Communication Server must be run as an application.

- Unless you are familiar with the download process, first read the section Download Panels and Locks Overview on page 1502.

From System Administration, complete the following steps:

1. From the ***Access Control*** menu, select ***Readers***.
   a. In the Readers listing window, sort the locks by the Initialization Required or Download Required columns, select one or more ILS offline/wireless locks, right-click on them, and then select **Download to Portable Device**.
   b. If the locks collectively belong to more than one (1) ILS offline panel, you will be prompted to select which panel to use for downloading to the Mobile Configurator.
2. (Optional) Select ***Access Panels*** from the ***Access Control*** menu.
   a. Click the ILS Offline or ILS Wireless tab.
   b. In the panel listing window, right-click on one (1) ILS panel, and then select **Download** to download the all of the locks assigned to that panel. ILS offline lock data is downloaded to the Mobile Configurator while ILS wireless lock data is sent to the locks via the Wireless Gateway.
3. (Optional) Open the system tree.
   a. From the ***View*** menu, select ***System Tree***, and then select an existing window or open a new one. Expand the Hardware node, and then the ILS panel icon to show the locks assigned to it.
   b. Right-click on one (1) ILS panel, and then select **Download** to download all locks assigned to the panel.
   c. (Optional) Select one or more ILS locks, right-click on them, and then select either **Download** (only available for wireless locks) or **Download to Portable Device**.

- **Download to Portable Device** - If the locks collectively belong to more than one ILS offline panel, you will be prompted to choose which ILS offline panel you want to use for downloading the lock information to the Mobile Configurator.
- **Download** - The wireless lock data is sent directly to the locks via their corresponding Wireless Gateway.

Note: Use the <Ctrl> key to multiple select locks in the system tree.

4. If the lock data was downloaded to the Mobile Configurator:
   a. Disconnect the Mobile Configurator from the workstation, and then connect it to the physical lock.
   b. Log onto the Mobile Configurator application using your operator ID and password, and then open the Mobile Configurator menu. For more information, refer to Add a Mobile Configurator Lock Operator on page 1498.
   c. (Optional) If this is the first time the lock will be updated, the lock was reset, or system-wide changes were made, select ***Initialize*** from the ***Lock*** menu, choose the lock from the list, and then click [Initialize Lock]. For more information, refer to Download System Settings on page 1486.
   d. If the lock does not need to be initialized, select ***Update*** from the ***Lock*** menu, choose the lock from the list, and then click [Update Lock] to transfer the system data from the Mobile Configurator to the lock.

Note: As the lock operator, you must have the ***Initialize*** or ***Update*** permission in order to perform the Initialize or Update operation at the lock using the Mobile Configurator. Any operation performed at the lock must have the corresponding operator permission enabled in OnGuard.

   e. Power off the Mobile Configurator and the power adapter, and then disconnect them from the lock.

View ILS Offline Lock Events

In order to view ILS offline lock events in Alarm Monitoring, the ILS offline operator must retrieve the events from the lock using the Mobile Configurator. Before using the Mobile Configurator to read the data at the lock, the system information must be downloaded from OnGuard to the Mobile Configurator to update the lock. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505.

When the Mobile Configurator is then connected to a workstation where Alarm Monitoring and Communication Server are running, the Mobile Configurator is used to upload the lock data to OnGuard. When this is completed, the lock events display automatically. For more information, refer to Upload ILS Offline Lock Events Using the Mobile Configurator on page 1507.

IMPORTANT: If you are using the Mobile Configurator with OnGuard on a Windows XP or Windows 2003 system, Communication Server must be run as an application.

Note: When you connect the Mobile Configurator to a workstation, that Mobile Configurator and all others, will show an online status in Alarm Monitoring.

In addition, the proper permissions must be configured for the Mobile Configurator operator to be able to upload the data from the lock. For more information, refer to Add a Mobile Configurator Lock Operator on page 1498.

Upload ILS Offline Lock Events Using the Mobile Configurator

Prerequisites: The Mobile Configurator is connected to a vacant USB port at a workstation where Microsoft Active Sync, OnGuard, and Communication Server are running.

IMPORTANT: If you are using the Mobile Configurator with OnGuard on a Windows XP and Windows 2003 systems, Communication Server must be run as an application.

From System Administration, complete the following steps:

1. Verify the operator permissions:
   a. From the ***Access Control*** menu, select ***Access Panels***.
   b. On the ILS Offline tab, select the Operators sub-tab.
   c. Ensure the **Read lock audits** permission is enabled for the ILS offline lock operator.

Note: As the lock operator, you must have the **Read lock audits** permission in order to get the events from the lock using the Mobile Configurator. Any operations performed at the lock must have the corresponding operator permissions enabled in OnGuard such as **Initialize**, **Update**, **Upload lock audits**, and **Upload PP audits** as well as **View lock audits** and **View PP audits**.

2. Download the lock information to the Mobile Configurator. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505.
3. Use the Mobile Configurator to update the locks:
   a. Disconnect the Mobile Configurator from the workstation, and then connect the power adapter to the ILS lock. Log onto the Mobile Configurator.
   b. Log onto the Mobile Configurator application using your operator ID and password, and then open the Mobile Configurator menu. For more information, refer to Add a Mobile Configurator Lock Operator on page 1498.
   c. (Optional) If this is the first time the lock is initialized, the lock was reset, or there were system-wide changes, select ***Initialize*** from the ***Lock*** menu, select the lock from the list, and then click [Initialize Lock]. For more information, refer to Download System Settings on page 1486.
   d. If the lock does not need to be initialized, select ***Update*** from the ***Lock*** menu, choose the lock from the list, and then click [Update Lock] to transfer the system data from the Mobile Configurator to the lock.
4. Use the Mobile Configurator to read the lock audits:
   a. From the ***Audits*** menu, select ***Read Audits > Read Lock Audits***:
      - From the list, choose the lock you are reading, and then use the Filter options to specify event types and/or date range.
      - Click [Read Audits]. Click [OK] when the read operation is completed.

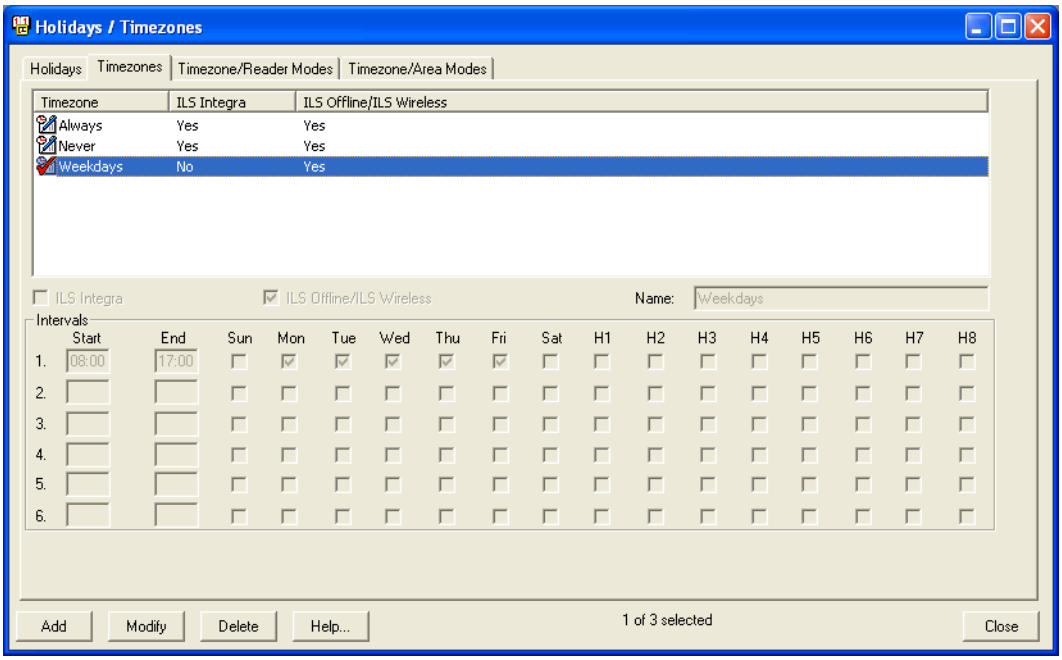
   IMPORTANT: You must perform the Read Lock Audits operation in order to get the lock events.

   b. From the ***Audits*** menu, select ***View Audits > View Lock Audits*** to ensure the information is valid. You can filter the lock audits such as Access Granted/Denied, and then click [View Audits] to display the events on the Mobile Configurator.
   c. From the ***Audits*** menu, select ***View Audits > View PP Audits*** to ensure the information is valid. You can filter the controller lock audits such as mode changes, and then click [View Audits] to display the events on the Mobile Configurator.

d. Disconnect the Mobile Configurator from the lock, and then connect it to the monitoring station.

5. Use the Mobile Configurator to upload the lock events to Alarm Monitoring:
   a. Connect the Mobile Configurator to a workstation where Alarm Monitoring and Communication Server are running.
   b. From the ***Upload*** menu, select ***Upload Audits*** > ***Upload PP Audits***, click [Upload], and then [OK] when the Mobile Configurator events are uploaded to the Mobile Configurator.
   c. From the ***Upload*** menu, select ***Upload Audits*** > ***Upload Lock Audits***, click [Upload], and then [OK] when the lock audits are uploaded to the Mobile Configurator.
   d. Log onto Alarm Monitoring. The lock and Mobile Configurator events are automatically displayed in the Main Alarm Monitor window.

ILS Offline/ILS Wireless Timezones Overview



Optionally, you can use the Timezones form to create timezones which will be downloaded to ILS offline/wireless locks. Each ILS Offline/ILS Wireless timezone consists of up to five (5) time range/day intervals. A maximum of 64 ILS Offline/ILS Wireless timezones are supported including the two (2) system time intervals, Always and Never.

ILS offline/wireless locks support a maximum of 100 holidays.

Note: An ILS Offline/ILS Wireless timezone must be associated with an ILS offline/wireless reader (lock) in order to assign it to Timezone/Reader Modes or Access Level configurations.

Add an ILS Offline/ILS Wireless Timezone

In System Administration, complete the following steps:

1. Select ***Timezones*** from the ***Access Control*** menu, and then select the Timezones tab.
2. Click [Add].

3. Select the **ILS Offline/ILS Wireless** check box to indicate this timezone is to be downloaded to ILS offline/wireless locks.
4. Type a name for the timezone in the **Name** field.
5. Define each time interval in this timezone, including the start and end times, the specific days of the week, and the holiday types you want. Enter **Start** and **End** times, and then select the check boxes you want the time range to apply to.
6. Click [OK].

ILS Timezone/Reader Modes Overview

Optionally, you can use the Timezones/Reader Modes form to configure up to 25 scheduled changes per lock. For more information, refer to Timezone/Reader Modes Form on page 711.

Examples of possible ILS offline/wireless configurations:

- 5 timezones containing 5 intervals each
- 10 timezones containing 2 intervals each and 1 timezone containing 5 intervals
- 25 timezones containing 1 interval each

Select Modes of Operation for ILS Locks during a Timezone

In System Administration, complete the following steps:

1. Select ***Timeszones*** from the ***Access Control*** menu.
2. On the listing window, select the reader (lock) you want to control the operation of during a particular timezone. This was the lock you added in the step: Add an ILS Offline Lock on page 1500 or Add an ILS Wireless Lock on page 1520.
3. Click [Modify].
4. Choose the timezone you want to configure for the selected reader (lock) such as an ILS Offline/ILS Wireless timezone you added in the step: Add an ILS Offline/ILS Wireless Timezone on page 1508.
5. In the Start section, from the drop-down, select the mode you want this lock to be placed into at the beginning of the selected timezone:
   - Card Only
   - Facility Code Only
   - Unlocked
   - First Card Unlock
6. In the End section, from the drop-down, select the mode you want this lock to be placed into at the end of the selected timezone.
7. Click [Assign]. The following things happen immediately:
   - The change is saved to the database.
   - The assignment window is updated.
   - For ILS wireless locks, the changes are downloaded to the wireless locks via the Wireless Gateway.
   - For ILS offline locks, the changes are not automatically downloaded. Instead, the lock is flagged for a download in the system hardware tree and the Readers and Doors folder.

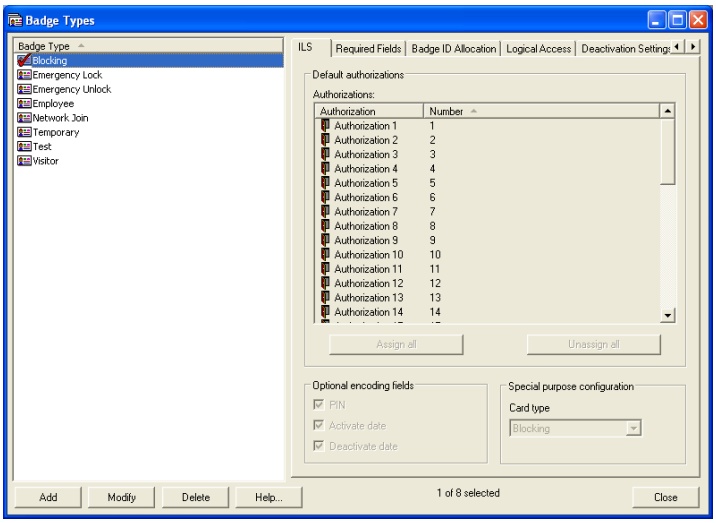
   Functionally, at the start of the selected timezone, the selected lock will begin to function in the selected **Start mode**. It will remain in that mode until the end of the timezone, at which time the lock will be placed in the selected **End mode**.

8. Repeat steps 4 - 7 for each additional timezone you want to configure for this lock.
9. Click [OK] to return to view mode. The listing window will be updated to reflect your changes.
10. Repeat this procedure if you want to set up the operating modes of other locks.
11. The changes must be downloaded from OnGuard to the ILS offline locks via the Mobile Configurator. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505.
12. (Optional) For ILS wireless locks, you can update the lock directly via the Wireless Gateway from Alarm Monitoring. For more information, refer to Update Wireless Reader Access Modes in the Alarm Monitoring User Guide.

Badge Types Folder - ILS Form

Optionally, you can configure the ILS badge types to:

- Encode authorizations for badge types that get assigned to cardholders.
- Specify the function of special purpose cards such as blocking or emergency unlock cards.



Configure ILS Badge Types

In System Administration, complete the following steps:

1. Select ***Badge Types*** from the ***Administration*** menu, and then select the ILS tab.
2. In the listing window, select the badge type you want to configure.
3. Select the authorization you want to assign as the default to a cardholder badge of this ILS badge type.
4. Select the options that you want to enable in the Optional encoding fields section of the window. For more information, refer to ILS Form on page 332.
5. Click [OK].

Note: To configure ILS special purpose badge types, refer to Configure Special Purpose Cards for ILS Offline/Wireless Locks on page 1511.

ILS Special Purpose Cards

IMPORTANT: Blocking cards for offline/wireless locks are not to be confused with blocking cards for Integra CT30 locks which have a different configuration. For more information about configuring an Integra blocking card, refer to Configure Blocking Cards for Integra Locks on page 1488.

Any card can be designated as a special purpose card. Special purpose cards are not added to the active badge count of the cardholder and all special purpose card types can be downloaded to the same lock.

ILS wireless locks support five (5) types of special purpose cards in the non-factory mode, including:

Blocking. When presented to the lock, and **Blocking override** is not enabled for the user, places the lock into the Blocked mode (denies access) or removes the lock from Blocked mode. It is not required to use the same blocking card that placed the lock in Blocked mode to remove the lock from Blocked mode.

Note: If a cardholder is assigned to a badge configured to override blocking, that badge will unlock a door that is blocked by a blocking card. For more information, refer to Add a Badge Template on page 199.

Emergency Lock. When presented to the lock, this card locks the lock and places the lock into Secured mode or removes the lock from Secured mode. It is not required to use the same Emergency Lock card that placed the lock into Secured mode to remove the lock from Secured mode.

Emergency Unlock. When presented to the lock, unlocks the lock and places the lock into Unsecured mode or removes the lock from Unsecured mode. It is not required to use the same Emergency Unlock card that placed the lock into Unsecured mode to remove the lock from Unsecured mode.

Network Join. When presented to the lock, prompts the lock to join the wireless network (Wireless Gateway).

Test. When presented to the lock, prompts the lock to issue a heartbeat signal to the Wireless Gateway in order to test the communications link between the Wireless Gateway and its lock.

IMPORTANT: The special purpose card needs to assigned to every lock to which it will be downloaded. To assign the card to the locks, an access level must be added that contains the locks, and then that access level is assigned to the card (badge) on the Cardholders folders > Access Level form. For more information, refer to Assign Access Levels to a Badge on page 118.

Configure Special Purpose Cards for ILS Offline/Wireless Locks

From System Administration, complete the following steps:

1. From the ***Administration*** menu, select ***Badge Types***.
2. Click [Add].
3. On the Badge Type tab:
   a. Enter a **Name** that describes the special function of the card such as `Emergency Lock`.
   b. From the **Class** drop-down, select “Special Purpose” to specify a badge that serves a special function such as blocking or unlocking a door in an emergency.

4. On the ILS tab, select the badge special function from the **Card type** drop-down such as "Emergency Lock." For more information, refer to ILS Form on page 332.
5. Click [OK]. The special badge type is now added to the Badge Type listing window.
6. (Optional) Repeat steps 2 - 5 to add other types of special purpose cards.
7. From the ***Administration*** menu, select ***Cardholders***.
8. Search for the cardholder record.
9. Add the special purpose card to the cardholder:
   a. From the **Badge type** drop-down, select the special purpose card.
   b. Select "Active" from the **Status** drop-down, and then click [OK].

Note: Special purpose cards are not added to the active badge count of the cardholder.

10. On the Access Levels tab:
    a. Click [Modify].
    b. Assign an access level to the special purpose card that contains the locks you want to block, put into the Secured or Unsecured mode, join to the Wireless Gateway, or test for Wireless Gateway communication.

IMPORTANT: ILS readers (locks) do not support assigning an access level to the card if that access level contains a lock that is in an access level already assigned to the card.

Note: You can assign access levels containing non-ILS readers because special purpose cards download to ILS locks, only. This allows you to define access levels for different locations, buildings, or regions, and create special purpose cards that will work for these areas.

    c. Click [OK].
11. Click [Print] to encode the blocking card using the printer/encoders listed in Required Printers/ Encoders on page 1487.
12. Download the special purpose card to the Mobile Configurator or Wireless Gateway and update the locks in your system. For more information, refer to Download Panels and Locks Overview on page 1502.

ILS iCLASS Printing and Encoding Overview

After the ILS system options have been configured, configure an encoder and a printer to print and encode the cards.

IMPORTANT: If you are encoding the ILS data to Book 1, the Lenel (iCLASS) card format must be specified with 16KBits/2Application Areas (Inside) or 16KBits/ 16Application Areas (Inside) for the memory configuration. In addition, when you encode to Book 1, 32K iCLASS cards are required. For more information, refer to Lenel (iCLASS) Card Format Form on page 275.

Required Encoders

The following devices are supported for encoding the ILS card data using the Lenel (iCLASS) smart card format:

- HID (iCLASS) encoder

Note: If you are encoding the ILS data to Book 0, use a card printer equipped with the HID (iCLASS) PROG encoder Rev.A. The HID (iCLASS) PROG encoder Rev.B can be used for encoding the ILS data to either Book 0 or Book 1. However, Rev.B is required for Book 1.

- DigiOn24 (iCLASS) encoder
- OMNIKEY (iCLASS) encoder

Note: If you are encoding the ILS data to Book 0, you can use any iCLASS encoder, however, Rev.B or later is required for Book 1.

OMNIKEY Encoders and 16kBit Cards

OMNIKEY (iCLASS) encoders do not support setting the HID key on Book 0, Page 0, App 1.

OMNIKEY encoders do not support formatting 16kBit cards to have eight (8) pages. Therefore:

- If you use pre-formatted cards: Select the memory configuration of those cards. The OMNIKEY encoder will handle it just fine.
- If you use blank cards: Select either 16KBits/2Application Areas (Inside) for 16kBit cards or 2kBits//2Application Areas (Inside) for 2kBit cards.

For more information, refer to Configure ILS Custom Encoding on page 1487.

Configure ILS iCLASS Printing and Encoding

In System Administration, complete the following steps to set up the encoder:

1. Select ***Workstations*** from the ***Administration*** menu. The Workstations folder opens.
2. Add and configure the workstation, and then click [OK].
3. Select the Encoders/Scanners tab.
4. Add the HID (iClass) PROG Rev.A/Rev.B encoder, and then configure it:
   a. On the General sub-tab, specify the encoder **Device type** as “HID iCLASS.”
   b. On the Location sub-tab, select the **This is a standalone device attached to this workstation** radio button.
   c. On the Communications sub-tab, select a vacant COM port.
   d. Click [OK].
5. Connect the HID (iClass) PROG Rev.A/Rev.B encoder to COM port on your workstation with a serial cable.

Printer/Encoder Setup

Complete the following steps to set up the printer such as the Magicard Rio 2 with an inline encoder:

1. Install the proper printer driver.
2. Connect the printer to a vacant USB port on your workstation and to the COM port using a serial cable.
3. In System Administration, select ***Workstations*** from the ***Administration*** menu.
4. Add and configure the workstation, and then click [OK].
5. Select the Encoders/Scanners tab.
6. Add the encoder, and then configure it:
   a. On the General sub-tab, specify the printer **Device type** as “Digion24 (iCLASS).”

b. On the Location sub-tab, select the **This is inline device that resides within a card printer attached to this workstation** radio button.

c. Select “Printer Series” in the **Card Printer** drop-down and “Contactless” in **Encoder Station** drop-down.

d. On the Communications sub-tab, select the COM port on your workstation where the printer is connected.

e. Click [OK].

ILS Reports Overview

From the Reports folder, use the Report Configuration or Reader Reports form to view or print the following ILS offline/wireless reports:

Report	Description
ILS Lock Authorizations By Cardholder	Lists ILS lock authorization levels assigned to the cardholder/badge, sorted by cardholder.
ILS Authorizations By Level	Lists ILS lock authorization levels assigned to the cardholder/badge, sorted by level.
ILS Lock Battery Status by Status	Lists ILS lock battery status, grouped by battery status (Low to High), wireless gateway, and battery percent.
ILS Lock Characteristics	Lists ILS lock configuration details by lock name.
ILS Lock Communications	Lists ILS wireless lock diagnostics by lock name.
ILS Lock Ownership	Lists the ILS locks owned by a cardholder.

This folder is displayed by selecting ***Reports*** from the ***Administration*** menu or by selecting the Reports toolbar button.

Toolbar Shortcut

For more information, refer to Chapter 8: Reports Folder on page 205.

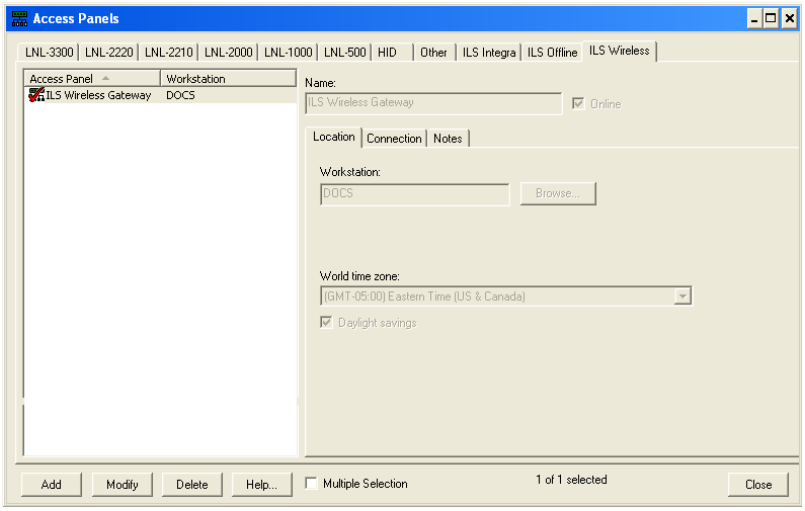
ILS Wireless Form

An ILS wireless device is a Wireless Gateway device that is treated as an access panel in OnGuard.

This form is used to:

- Assign names to ILS wireless access panels in the software.
- Specify access panel setup parameters.
- Specify communication panel setup parameters, including the workstation associated with the panel.

ILS Wireless Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name the ILS Wireless access panel (Wireless Gateway). This is a “friendly” name assigned to each Wireless Gateway to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel will be online. **Online** indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Select the workstation or server to which the Wireless Gateway is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations. You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

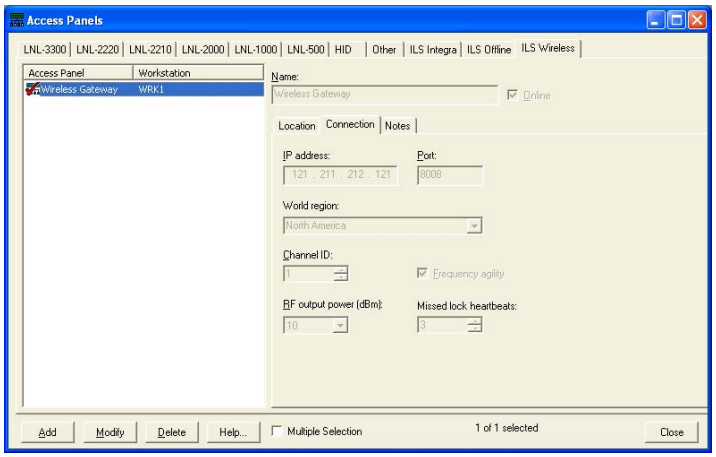
Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click the [OK] button to then enter the workstation name in the **Workstation** field.

Daylight savings

Select this check box if Daylight Saving Time is enforced in the selected access panel’s geographical location.

ILS Wireless Form (Connection Sub-tab)



IP Address

This is the Internet Protocol (TCP/IP) address of the Wireless Gateway device. The IP address entered here must be unique across all ILS wireless panels for both the primary and secondary IP addresses. An IP address consists of four (4) numbers, each in the range of 0 - 255. A period separates each number. The Mobile Configurator must be configured to have the same IP address as what you enter in this field. Refer to the ILS Lock Operation User Guide to program the IP address for the Mobile Configurator.

Port

The **Port** is pre-defined to `8008`. SSL (Secure Sockets Layer) protocol with mutual authentication is used during communications between OnGuard and the ILS Wireless Gateway device.

World region

Specifies the region where the Wireless Gateway is installed.

The **World region** setting determines the frequency bands and, subsequently, the **Channel ID** values available for the Wireless Gateway. This information is derived from the varying standards and regulations for wireless communications in different regions of the world.

- "North America" supports Channel IDs from 1 - 26.
- "European Union" supports Channel IDs from 1 - 20.

Selecting the **World region** also ensures the appropriate firmware is downloaded to the WLM and WWM. If you modify **World region**, make sure to download the WLM and WWM firmware. For more information, refer to Download ILS Wireless Firmware on page 1524.

The **World region**, **Channel ID**, and **RF output power** settings apply to both the Wireless Gateway and its associated locks.

Channel ID

Specifies the channel number of the Wireless Gateway from 1 - 26 with a default value of 1. This channel is used by the Wireless Gateway to communicate to its associated locks.

When placing several Wireless Gateways in close proximity where there is overlapping RF coverage, make sure to configure each of the Wireless Gateways with a unique **Channel ID**. Even when **Frequency agility** is enabled, the locks will use the initial **Channel ID** of the Wireless Gateway to which they are assigned, and if multiple Wireless Gateways use the same **Channel ID**, and are in range of the locks, the locks will attempt to communicate to the Wireless Gateways

using the same channel. This may cause the channel to become overcrowded resulting in unreliable communication (retries and frequency hopping).

If you change the **Channel ID**, this will affect the communication between the Wireless Gateway and its associated locks, so you should update the locks using the Mobile Configurator. Optionally, if you are only changing the **Channel ID**, and **Frequency agility** is enabled on all of the Wireless Gateway's locks, rather than updating the locks, you could allow the locks to find the new Wireless Gateway channel. However, whenever one of these locks tries to join a Wireless Gateway, it will always begin searching from the old channel. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505.

Frequency agility

Allows the Wireless Gateway to self-adjust dynamically when RF (Radio Frequency) interference is encountered from another device by hopping (switching) to a "quieter" location in the bandwidth to transmit the data. The Wireless Gateway will hop to the next higher channel in the bandwidth after five (5) retries. RF interference may cause unreliable communication (retries and frequency hopping).

If you change the lock's **Frequency agility**, you will need to update the lock using the Mobile Configurator. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505.

RF output power (dBm)

Specifies the RF (Radio Frequency) power. Choices include:

- 0 dBm
- 5 dBm
- 10 dBm
- 15 dBm

dBm refers to the power level of the signal strength expressed in decibels above 1 milliwatt.

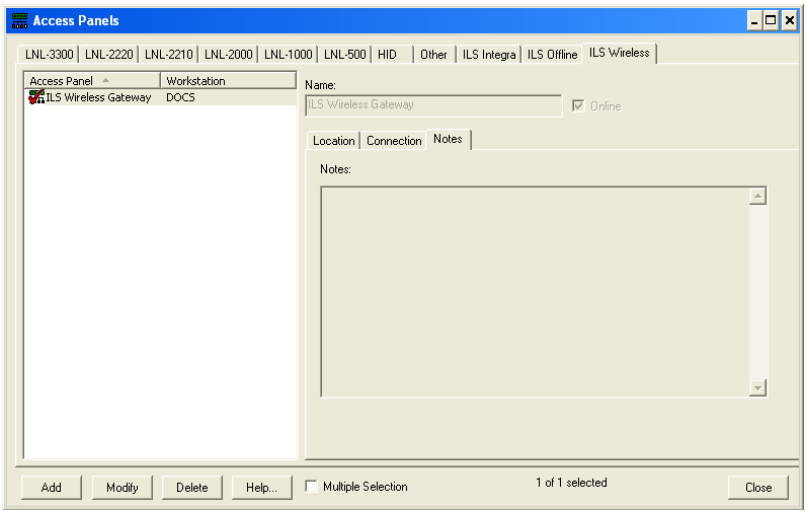
You may need to adjust the **RF output power** to achieve the signal strength required at your site. For example, higher power levels are required as the distance between the lock and Wireless Gateway is increased or if the signal must travel through a thick wall. However, lower power levels will extend the lock battery life.

If you change the lock's **RF output power**, you will need to update the lock using the Mobile Configurator. For more information, refer to Download ILS Offline/Wireless Locks from System Administration on page 1505.

Missed lock heartbeats

Specifies the number of missed lock heartbeats allowed before an alarm generates. Missed lock heartbeats can be configured from 1 - 5 with a default value of 1.

ILS Wireless Form (Notes Sub-tab)



Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the View Notes procedure in the Monitor Devices chapter in the Alarm Monitoring User Guide.

Configure an ILS Wireless Locking System

Configuring an ILS wireless system in OnGuard requires the use of an ILS wireless device to transmit data from OnGuard to the ILS locks and vice versa. In order to configure an ILS wireless system in OnGuard you must first add an ILS wireless panel (Wireless Gateway), and then define the locks to which the data is downloaded and from which events are retrieved via the Wireless Gateway. For information on the Wireless Gateway, refer to the ILS Lock Operation User Guide.

To configure an ILS wireless system, complete the following steps:

1. Add an ILS Wireless Access Panel on page 1519.
2. Add an ILS Wireless Lock on page 1520.
3. Modify ILS Wireless Panel Assignment on page 1522.
4. Configure ILS System Options on page 1522.
5. Configure ILS Custom Encoding on page 1487.
6. Configure ILS iCLASS Printing and Encoding on page 1513.
7. Configure ILS Badge Types on page 1510.
8. Configure Special Purpose Cards for ILS Offline/Wireless Locks on page 1511.
9. Add an ILS Offline/ILS Wireless Timezone on page 1508.
10. Select Modes of Operation for ILS Locks during a Timezone on page 1509.
11. Configure the ILS Cardholder Authorization Assignments on page 1491.
12. Configure ILS Priority One Events on page 1524.

ILS Wireless Lock Processing

After your system is up and running...

When the configuration of an ILS wireless lock is changed in OnGuard (such as reader settings, cardholders, timezones, etc.) and the lock is currently offline, the lock will be automatically updated when it goes online. You will also need to download the relevant configuration data stored in the OnGuard database to the ILS hardware (Wireless Gateways and wireless locks) and upgrade the ILS wireless firmware as needed. For more information, refer to the sections Download ILS Offline/ Wireless Locks from System Administration on page 1505 and Download ILS Wireless Firmware on page 1524.

From Alarm Monitoring, you can do the following:

- Update reader access modes.
- Issue a command to download ILS wireless locks.
- Monitor ILS wireless lock events that are sent wirelessly or retrieve these events by issuing a command to read the audits. For more information, refer to the sections Monitor ILS Wireless Lock Events on page 1524 or Retrieve ILS Wireless Lock Events in the Alarm Monitoring User Guide.
- Check that the Wireless Gateway and its ILS wireless locks can communicate. For more information, refer to View Wireless Diagnostics Information in the Alarm Monitoring User Guide.
- View lock status information. For more information, refer to View Wireless Lock Information in the Alarm Monitoring User Guide.

ILS Wireless Lock Panel Overview

The ILS wireless lock panel actually refers to a Wireless Gateway device. The fields configured here deal directly with the ILS wireless device. These settings are communicated to the Wireless Gateway as well as each ILS wireless lock assigned to it except for **RF output power** which is independent of the Wireless Gateway and its locks.

IMPORTANT: Configure the Wireless Gateway panel settings before adding cardholder records to the database. Changing the Wireless Gateway panel settings after cardholder records are added will result in a full cardholder database download to the Wireless Gateway.

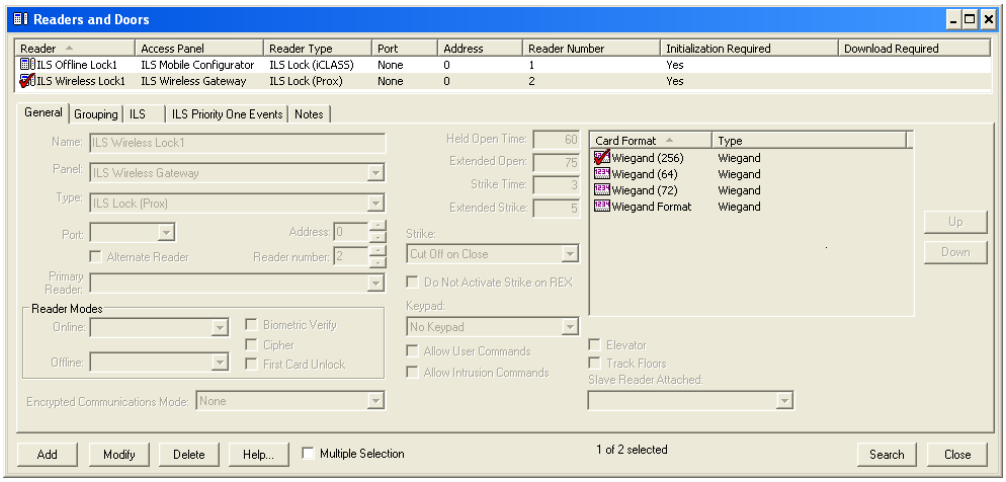
Add an ILS Wireless Access Panel

In System Administration, complete the following steps:

1. From the ***Access Control*** menu, select ***Access Panels***, and then select the ILS Wireless tab.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the ILS wireless panel.
4. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system or defining panels, but instead would wait until you're ready to put the panel into service.
5. On the Location sub-tab, configure the **Workstation**, **World time zone**, and **Daylight savings** settings. To review specifics regarding these fields see the ILS Wireless Form (Location Sub-tab) on page 1515.

6. On the Connections sub-tab, configure the **IP Address**, **SSL port**, **Channel ID**, **Frequency agility**, **RF output power**, and **Missed lock heartbeats** settings. To review specifics regarding these fields see the ILS Wireless Form (Connection Sub-tab) on page 1516.

ILS Wireless Lock Overview



To add an ILS wireless lock you must first add an ILS wireless lock panel. Adding an ILS wireless lock is much like adding a reader for OnGuard with the exception of not having full access to all of the options as they are not supported by ILS wireless locks. Fields not supported for ILS wireless locks will not be unavailable.

When you add an ILS wireless lock, the **Name**, **Panel**, **Type**, **Held Open Time**, **Extended Open**, **Strike Time**, and **Extended Strike** fields will be activated. **Extended Strike** and **Extended Open** are typically used with the ADA feature. However, if **Lock when lever is released** is enabled for the lock, the lock will re-engage after the cardholder turns the lever. Configure this and the other ILS-specific lock options on the Readers folder ILS form. For more information, refer to ILS Form on page 677.

Card formats for ILS locks are selected for specific lock types, and can be prioritized and sorted. For more information on card formats, refer to Lock Card Formats on page 1499.

Notes: Reader numbers (lock IDs) are unique across an Enterprise system for ILS locks.

Although not available when adding the lock, reader (lock) modes can be configured for the start and end of a timezone. For more information, refer to Select Modes of Operation for ILS Locks during a Timezone on page 1509.

If you change reader mode settings, the lock must be updated from Alarm Monitoring. For more information, refer to Update Wireless Reader Access Modes in the Alarm Monitoring User Guide. Alternatively, you can update the lock by downloading the lock information to the Mobile Configurator.

Add an ILS Wireless Lock

Note: Optionally, you can configure multiple ILS wireless locks using the ***Application*** > ***Wizards*** menu option in System Administration. For more information, refer to Application Menu on page 60.

In System Administration, complete the following steps:

1. Select ***Readers and Doors*** from the ***Access Control*** menu. The Readers folder opens.
2. On the General tab, click [Add].
3. In the **Name** field, enter a unique, descriptive name for the reader.
4. In the **Panel** field, select the access panel to which you want to connect the reader. This is the ILS Wireless access panel (Wireless Gateway) you added in the step: Add an ILS Wireless Access Panel on page 1519.
5. In the **Type** field, select the lock type. Choices include:
   - ILS Lock (Magnetic)
   - ILS Lock (iCLASS)
   - ILS Lock (MIFARE)
   - ILS Lock (Prox)

Note: When the lock type is selected, this determines which card formats are available for assignment to the lock.

6. Select one or more card formats.

Note: ILS supports up to four (4) Wiegand card formats for iCLASS, MIFARE, and proximity type locks and, depending on your version of OnGuard, up to four (4) smart card formats for iCLASS and MIFARE locks, only.

   - If you selected “ILS Lock (Magnetic)” the card format is automatically assigned.
   - For iCLASS locks, you must select at least one card format from the Smart Card Formats sub-tab (iCLASS) AND the appropriate Wiegand card formats from the Access Control Card Formats sub-tab. Smart card formats supported by the ILS ICLASS locks include Lenel (iCLASS). For more information, refer to Add a Lenel (iCLASS) Smart Card Format on page 276.
   - For proximity locks, select the appropriate Wiegand card formats from the Access Control Card Formats sub-tab, only.
   - (Depending on your version of OnGuard, this option may not be available.)
     For MIFARE locks, you must select at least one MIFARE card format from the Smart Card Formats sub-tab AND the appropriate Wiegand card formats from the Access Control Card Formats sub-tab. Smart card formats supported by ILS MIFARE locks include Smart Card CSN and Lenel (MIFARE). For the Smart Card CSN card format, “ISO 14443A” must be configured as the **Credential Type**. For more information, refer to Add a Smart Card CSN Card Format on page 279 and Add a Lenel (MIFARE) Smart Card Format on page 277.

7. Prioritize the card formats as required. For more information, refer to Card Format on page 640.
8. Configure the remaining settings as required.
9. (Optional) On the Grouping tab, configure the reader (lock) group settings. For more information, refer to Grouping Form on page 643. When group settings are configured, you can filter the locks displayed in the listing window using the reader search function. For more information, refer to Search for Readers by Groups on page 644.
10. On the ILS tab, configure the options as required. For more information, refer to ILS Form on page 677.
11. (Optional) On the ILS Priority One Events tab, if you want to assign priority one events to the lock, complete the following steps. For more information, refer to ILS Priority One Events Form on page 681.
    a. Click [Modify].
    b. From the Available list, select the events you want to specify as priority one.

c. Click [Assign] to move the events to the Selected list.

d. (Optional) From the Selected list, select priority one events, and then click [Remove] to remove these events from priority one status.

e. Click [OK].

Note: After the lock is added, it will be flagged automatically for "Initialization Required."

Modify ILS Wireless Panel Assignment

Prerequisites: Ensure you are in single selection mode.

Note: Locks assigned to ILS wireless panels can be reassigned to a different ILS wireless panel within the same segment. When you reassign an ILS wireless lock to a different ILS wireless panel, the diagnostic information for the lock is cleared. For more information, refer to View Wireless Diagnostics Information in the Alarm Monitoring User Guide.

In System Administration, complete the following steps:

1. From the ***Access Control*** menu, select ***Readers***. The Readers folder opens.
2. From the list, select the lock you are changing.
3. On the General tab, click [Modify].
4. In the **Panel** field, select the ILS wireless panel to which you want to reassign the lock.
5. Click [OK].

Modify ILS Wireless Lock Type

After a lock is added, you can modify the lock's **Type** to accommodate upgrades or changes to the lock's card technology such as changing from a magnetic lock to a proximity lock or from a proximity lock to an iClass lock. This change also requires that you select card formats for the new lock type.

Note: Reader (lock) type has an impact on battery life. Proximity and iCLASS reader field excitation enters a low power mode when no card is present.

System Options Folder - ILS Form Overview

After the ILS lock panel and reader (lock) have been added and configured, you must configure the ILS system options.

Use the ILS form to configure data elements that affect the programming of all ILS controllers and locks that exist in the system.

IMPORTANT: When you modify certain system settings, you must download this information to the Mobile Configurator to update or initialize the lock. For more information, refer to Download System Settings on page 1486.

Configure ILS System Options

In System Administration, complete the following steps:

1. Select ***System Options*** from the ***Administration*** menu, and then select the ILS tab. For more information about the settings configured in this procedure, refer to the ILS Form on page 419.

2. Click [Modify].
3. In the **System code** field enter the system code. This is simply a unique identifier much like a name.
4. In the **Codes look ahead** field, enter the number of codes you want to apply to all readers (locks) in the system.
5. Select the **Lock or card date precedence**.
6. Specify the format to **Store badge activate/deactivate dates**. Choices include:
   - None
   - Date only
   - Date and time
7. Specify the amount of days to keep old wireless diagnostics data in the **Clean up wireless diagnostics after (days)** field. For more information, refer to View Wireless Diagnostics Information in the Alarm Monitoring User Guide.
8. In the **Number of general authorizations** field, enter the number of authorization that will be available for assignment.
9. (Optional) Double-click on any default Authorization item in the list window, and then type a unique name if required.
10. To enable the Alternative Fire Code (AFC) functions on a door-by-door basis, select the **Manage Alternative Fire Code (AFC)** check box.
    a. To allow a relocking timers to be set to relock doors after they are unlocked, select the **Manage relock timer** check box.
    b. To allow individual locks to be locked automatically when the deadbolt is engaged, select the **Relock with deadbolt mode** check box.
11. Click [OK].

ILS Priority One Events Overview

You can specify up to 20 ILS wireless lock events as priority one events. Priority one events are transmitted immediately from the lock via the Wireless Gateway to Alarm Monitoring as these events occur.

- In the Alarm Configuration folder, use the ILS Priority One Events form to configure priority one events on a system-wide basis. By default, all ILS wireless locks use these system priority one events. For more information, refer to ILS Priority One Events Form on page 879.
- In the Readers folder, use the ILS Priority One Events form to configure priority one events on a lock-by-lock basis. For more information, refer to ILS Priority One Events Form on page 681.

Note: Some events are pre-defined as priority one and are therefore not in the Available list. These events include: Reader Firmware Upgraded, ACU Firmware Upgraded, WLM Firmware Upgraded, and Audit Trail Limit Reached.

IMPORTANT: Use care as to how many and which events you select as priority one events. With careful configuration of the priority one events, the lock's battery life may be extended by selecting events that are important but not frequently received. However, if you select events that are not critical and are likely to be generated frequently, the batteries will drain more quickly and need to be replaced more often.

Non-priority one events are sent at the heartbeat after the **Request audits** interval. For information on configuring the interval, refer to the ILS Form on page 677. In addition, you can retrieve non-priority

lock events by issuing the Read Audits command from Alarm Monitoring. For more information, refer to Retrieve Wireless Lock Events in the Alarm Monitoring User Guide.

Configure ILS Priority One Events

In System Administration, complete the following steps to configure the system priority one events:

1. Select ***Alarms*** from the ***Monitoring*** menu. The Alarm Configuration folder is displayed.
2. On the ILS Priority One Events tab:
   a. From the Available list, select the events you want to specify as priority one. For more information, refer to ILS Priority One Events Form on page 879.
   b. Click [Assign] to move the events to the Selected list.
   c. (Optional) From the Selected list, select priority one events, and then click [Remove] to remove these events from priority one status.
   d. Click [OK].

In System Administration, complete the following steps to configure priority one events for the lock:

1. Select ***Readers*** from the ***Access Control*** menu. The Readers folder is displayed.
2. Select the ILS wireless lock for which you want to configure the priority one events.
3. On the ILS Priority One Events tab:
   a. From the Available list, select the events you want to specify as priority one. For more information, refer to ILS Priority One Events Form on page 681.
   b. Click [Assign] to move the events to the Selected list.
   c. (Optional) From the Selected list, select priority one events, and then click [Remove] to remove these events from priority one status.
   d. Click [OK].

Download ILS Wireless Firmware

IMPORTANT: Be sure to use the most current version of the firmware.

Wireless communication between OnGuard and ILS wireless locks is accomplished through the Wireless Gateway. Within the Wireless Gateway there are two (2) micro-controllers:

- Wireless WAP Module (WWM)
- WAP Main Controller (WMC)

The ILS wireless lock contains a reader unit and two (2) micro-controllers:

- Access Control Unit (ACU)
- Wireless Lock Module (WLM) - This is the radio unit.

The firmware for all of these controllers and the reader are downloaded from Alarm Monitoring. For more information, refer to Download ILS Wireless Lock Firmware in the Alarm Monitoring User Guide.

Note: Reader firmware is not available for magnetic type locks.

Monitor ILS Wireless Lock Events

ILS wireless lock events are reported in Alarm Monitoring by way of three (3) different mechanisms:

- Priority one events are sent immediately as soon as these events occur at the lock. For more information, refer to ILS Priority One Events Overview on page 1523.
- Non-priority events are retrieved at configurable intervals, and then sent at the next heartbeat. For more information, refer to the **Request audits** option in the ILS Form on page 677.
- From Alarm Monitoring, you can request to have the non-priority events sent at the next heartbeat by issuing the Read Audits command. For more information, refer to Retrieve ILS Wireless Lock Events in Alarm Monitoring User Guide.

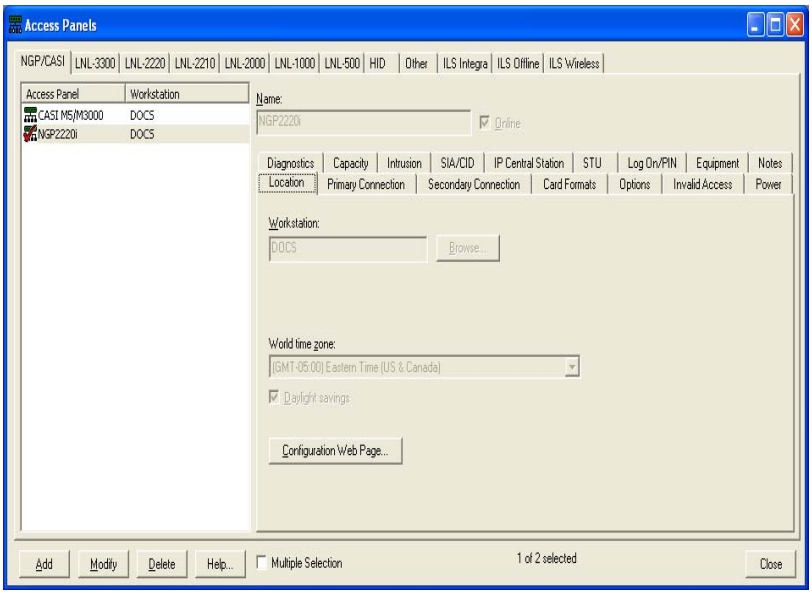
APPENDIX L

NGP Access Panel Configuration

Configuring an NGP Access panel requires configuring the network settings and configuring the OnGuard software. OnGuard allows you to set up an access control and intrusion system using the NGP access panel. A system that utilizes NGP can specify specific profiles, areas, users, and door/readers to create a access control and/or intrusion based system.

IMPORTANT: When adding NGP hardware to the system make note of the serial ID number listed on the hardware itself. You must know these ID numbers when configuring the software.

NGP/CASI Form (Location Sub-tab)



Listing window

Lists currently defined access panels and the name of the workstation that is connected to each.

Name

Enter a name for the panel type. This is a “friendly” name assigned to each panel to make it easy to identify. Each name must be unique and can contain no more than 32 characters.

Online

If selected, the panel will be online. Online indicates that the panel is ready for use, and that the Communication Server will attempt to communicate with the panel. If the panel is not marked as online, the Communication Server will not attempt to communicate with the panel.

Workstation

Selects the workstation to which the access panel is or will be connected in order to transfer events/commands. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Note: You are required to enter the workstation’s NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.f)

Browse

Displays a Browse for Computer window from where you can click on the name of a workstation to highlight the entry. Click [OK] to then enter the workstation name in the **Workstation** field.

World time zone

Select the world time zone for the selected access panel’s geographical location. The selections in the drop-down list are listed sequentially, and each includes:

- The world time zone’s clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England.
- The name of one or more countries or cities that are located in that world time zone.

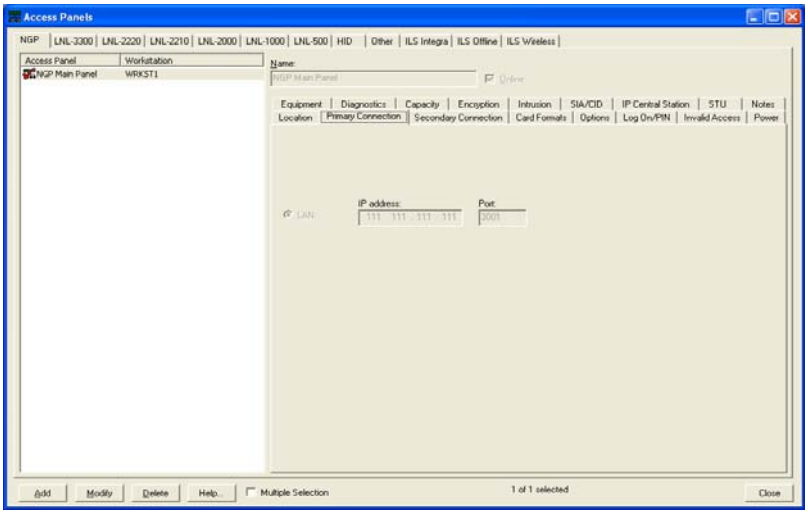
Daylight savings

Select this check box if Daylight Saving Time is enforced in the selected access panel’s geographical location.

Configuration Web Page

Opens the web page used to configure the access panel. Only available when in view mode and if the controller has an IP address or host name configured for the primary connection.

NGP Form (Primary Connection Sub-tab)



LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's IP address or Host name.

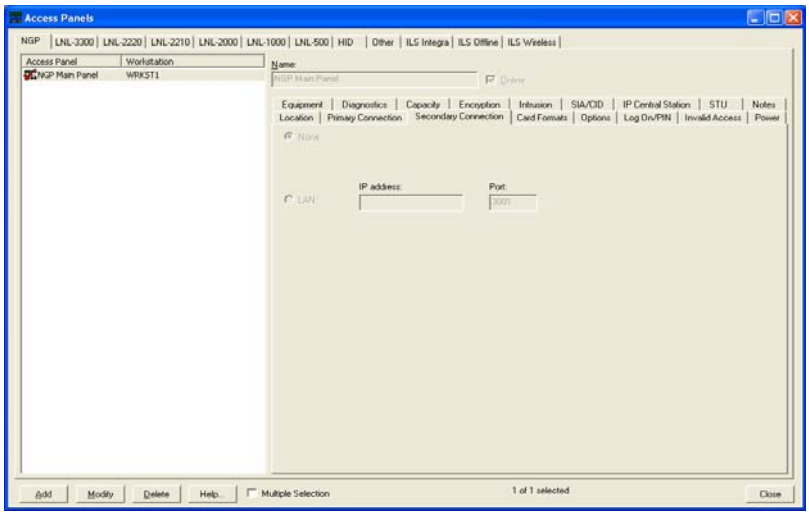
IP address

If you selected the **LAN** radio button, enter the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

Port

The network port that the LAN connection will be established on. The default is 3001.

NGP Form (Secondary Connection Sub-tab)



None

Select this radio button if the panel does not use a secondary connection.

LAN

Select this radio button if the workstation will communicate with the access panel over a Local Area Network. You must also specify the workstation's IP address or Host name.

IP address

If you selected the **LAN** radio button, enter here the Internet Protocol (TCP/IP) address for the access panel, as provided by your LAN Network Administrator. An IP address consists of four numbers, each in the range of 0 through 255. A period separates each number. The access panel itself must be configured to have the same IP address as what you enter in this field. Refer to the Hardware Installation Guide to program the IP address for the access panel.

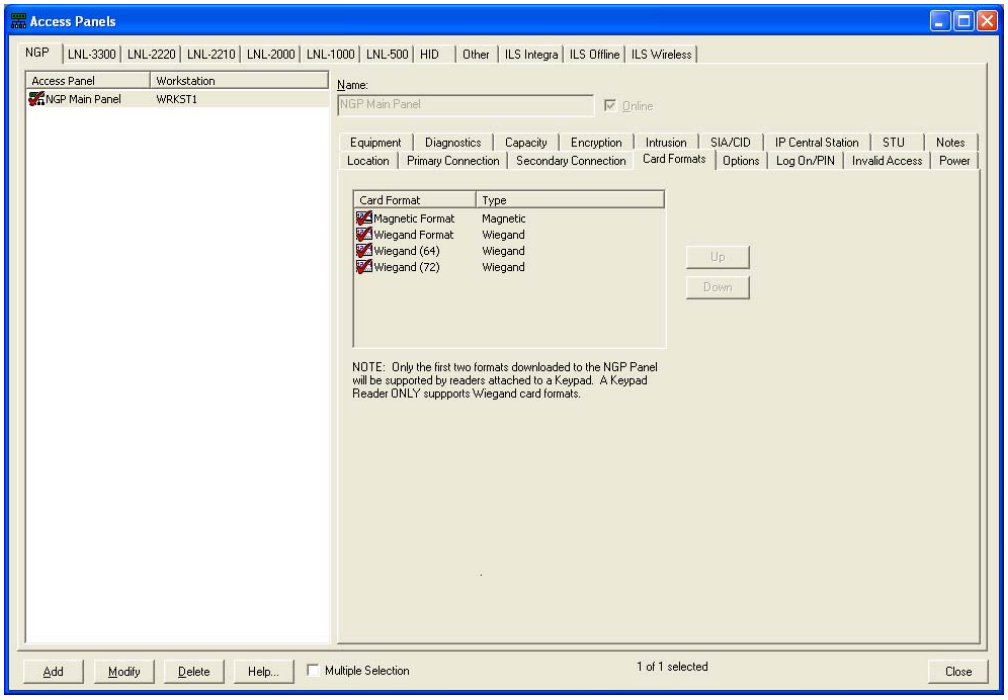
Baud Rate

If you selected the **LAN** radio button, a read-only field that shows the baud rate of your LAN connection.

Port

The network port that the LAN connection will be established on. The default is 3001.

NGP Form (Card Formats Sub-tab)



Card Format listing window

Lists all card formats currently available for the panel. De-select any format that you do not want the panel to use.

Note: Readers attached to a keypad only support the first two (2) formats downloaded to the NGP panel and Wiegand card formats.

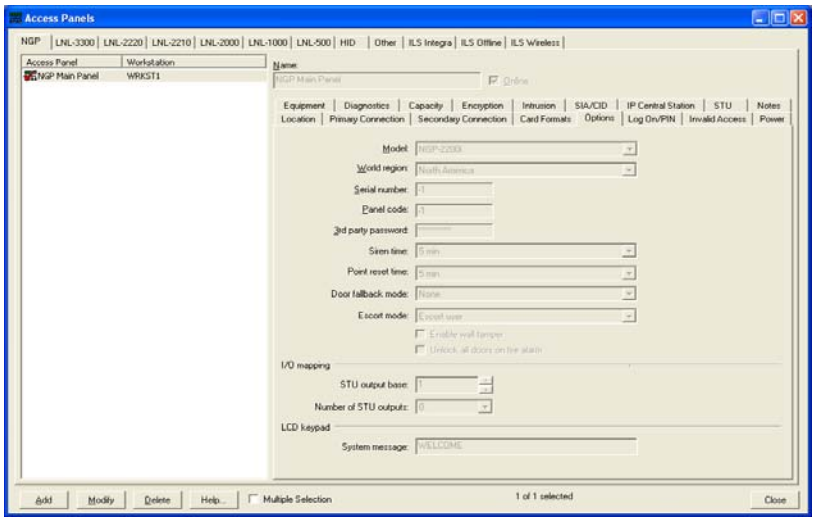
Up

With the card formats selected, click [Up] to move the selections to the top of the list.

Down

With the card formats selected, click [Down] to move the selections to the bottom of the list.

NGP Form (Options Sub-tab)



Model

Select the correct model of the panel used in the system.

Note: When you add CASI access panels, alarm panels may be automatically assigned to them depending on the model.

- **DirecDoor**: One onboard alarm panel is automatically assigned. A second alarm panel is automatically assigned if "DDIO" is specified for the panel's slot configuration.
- **M5/M3000**: One alarm panel is automatically assigned for each 20DO/16DI slot assignment. For more information about slot assignment, refer to NGP Form (Slots) on page 1547.

Model	Alarm Panel	Maximum Inputs/Outputs
DirecDoor	DirecDoor Onboard	Supports up to 6 outputs
	DirecDoor DDIO	Supports up to 4 inputs and 4 outputs
M5/M3000	One M5/M3000 20DI per 20DI board	Supports up to 20 inputs
	One M5/M3000 16DO per 16DO board	Supports up to 16 outputs

- **M2000**: Independent of slot assignment, two alarm panels are automatically assigned when this panel is added.

Model	Alarm Panel	Maximum Inputs/Outputs
M2000	M2000 8DO	Supports up to 8 outputs
	M2000 10DI	Supports up to 10 inputs

World region

Select the region of the world where the panel is used. Depending on the region selected, some options may or may not be available.

Serial number

Enter the serial number of the specific panel. This allows the software to identify each panel. The serial number is silk-screened on the back of the SOM Module and will contain the following: 4 Numeric Digits, 1 Alpha Digit, and then 6 Numeric Digits. It is these last 6 Numeric Digits that need to be entered into this field. The Serial Number of the SOM board MUST match the Serial Number entered here for authenticated communications.

Panel code

This is a reference number to identify the panel, site, or account. For a new panel, this can be any non-zero number and can be the same for all panels per site or per account if desired. The panel code entered through the panel's web page MUST match the panel code entered here for authenticated communications.

3rd Party Password

A security key used by the software to block an unauthorized connection to the panel. For a new panel this can be set as desired. The panel code entered through the panel's web page MUST match the panel code entered here for authenticated communications.

Siren time

Select the duration for any siren activations for the panel.

Point reset time

Select the duration for which all input points that are tripped momentarily will be treated as an alarm.

Door fallback mode

Select the cardholder that are to be granted access if the door controller is unable to communicate with the main panel.

- **None** - No cards are accepted.
- **Valid card format** - All readable cards are accepted.
- **Valid facility code** - All cards with the correct site code are accepted.

Escort mode

Select the type of user who are able to escort visitors.

- **Escort user** - Valid users with escort privileges.
- **Any user** - Any valid user either permanent or temporary.

Enable wall tamper

Enable to monitor the wall tamper of the main board.

Unlock all doors on fire alarm

Enable to unlock all of the doors when a fire alarm is activated.

STU output base

Select the number of the first programmable output to be reserved for use with a parallel STU.

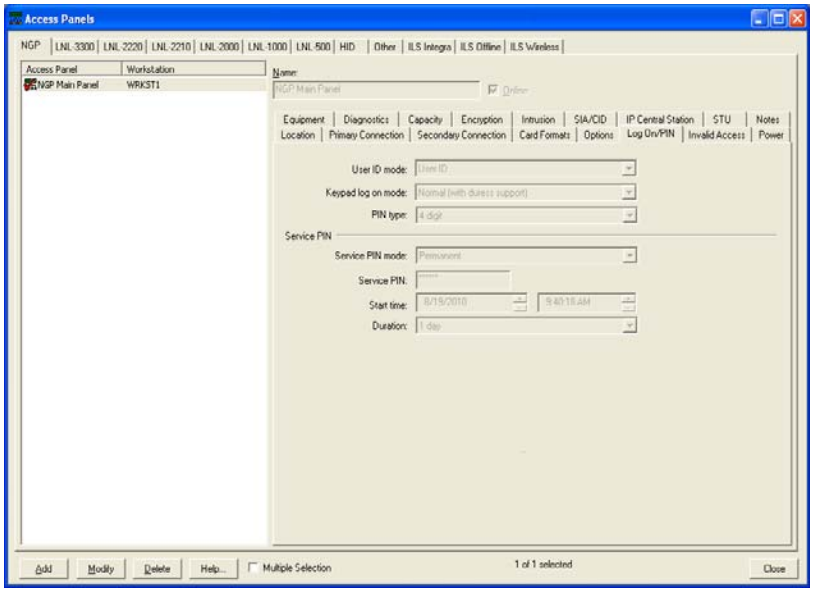
Number of STU output

Select the number of STU outputs for the system.

System message

A greeting of up to 16 characters to appear at the LCD display.

NGP Form (Log on/PIN Sub-tab)



User ID mode

Select the number of digits used for the badge number.

Keypad log on mode

Select the mode used to log into the system. The choices are:

- **Normal** - The keypad is used normally.
- **Normal (with duress support)** - The keypad can be used to signal a duress.
- **PIN only** - You can only log in with a PIN.
- **PIN only (allow duplicates)** - You can only log in with a PIN but people can use duplicates PIN numbers.

PIN type

Select the PIN length used for cardholders.

Service PIN mode

Controls the PIN used for access to the panel by service personnel. It is only usable when the panel cabinet is opened. Choices are:

- **Permanent** - Sets the service PIN on the panel to the value in the Service PIN field.
- **Temporary** - Sets the service PIN on the panel to the value in the Service PIN field. This PIN will be valid from the date/time in the 'Start Time' fields for the duration listed in the Duration field.

Service PIN

Enter a service PIN. The service PIN is needed when the Service PIN mode field is set to be either “Permanent” or “Temporary” and must be entered when services the panel.

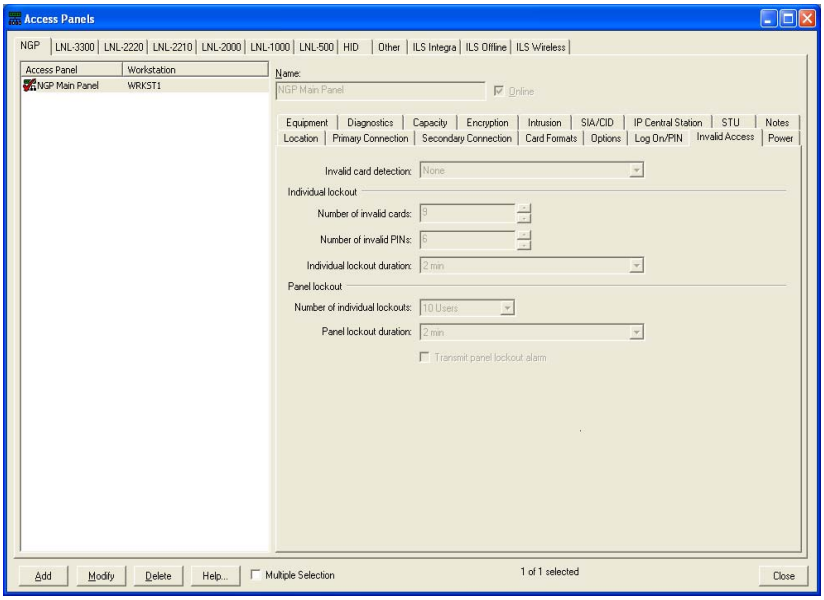
Start time

Enter the start date and time that the “Temporary” service PIN will be valid. Use in conjunction with the Duration field to set how long the PIN is valid for.

Duration

Set the time that the “Temporary” service PIN is valid for.

NGP Form (Invalid Access Sub-tab)



Invalid card detection. Select the type of invalid card detection. Choices are:

- **None** - Does not detect invalid cards.
- **Invalid cards only** - Cards that are denied access due to being: not in the database, wrong facility code, or wrong issue code.
- **Invalid cards and high risk denied** - Cards that are denied access due to being an: invalid card AND: Card expired, schedule expired, Interlock violation, Reader locked out, wrong area.
- **Invalid cards and all denied** - Cards that are denied access due to Invalid card or any reason.

Number of invalid cards

Set the number of invalid card attempts before the user is locked out of the system.

Number of invalid PINs

Set the number of invalid PIN attempts before the user is locked out of the system.

Individual lockout duration

Set the length of time that a user is locked out of the system after a user-defined number of invalid card or PIN attempts.

Number of individual lockouts

Set the number of users that can be locked out of the system before the panel is locked for further use.

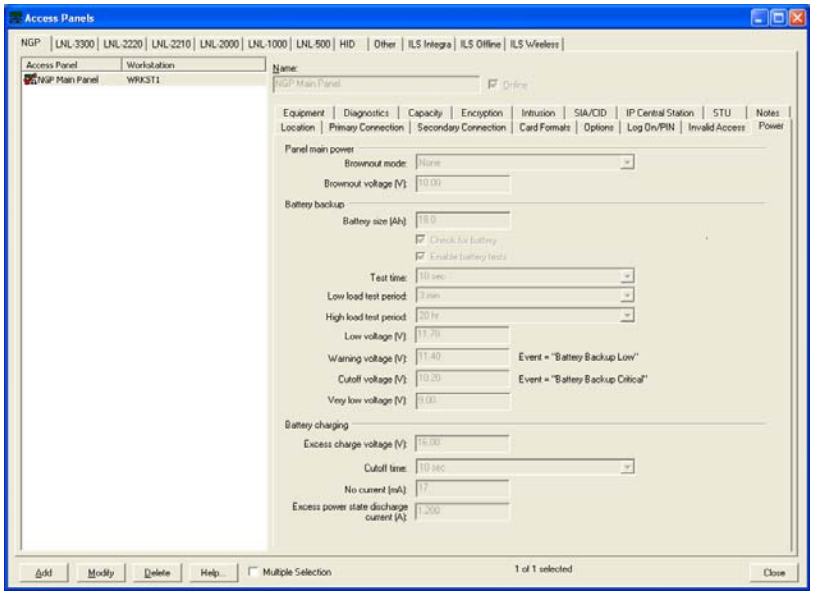
Panel lockout duration

Set the length of time the panel will be locked after the user-defined number of lockouts occurs.

Transmit panel lockout alarm

Enable to send an alarm when the panel is locked out.

NGP Form (Power Sub-tab)



Brownout mode

Set the reaction to a reduced AC voltage. Choices are:

- **Local alarm** - sends an alarm.
- **Alarm and report** - sends an alarm and creates a report.
- **Report only** - creates only a report.

Brownout voltage (V)

Set the voltage level considered to be a brown out.

Battery size (Ah)

Set the amp-hour rating for the panel's backup battery.

Cutoff time

Used when there is excessive battery voltage. If excessive voltage is detected, the battery is disconnected for the cut off time (default of 10sec) and then reconnected when this time elapses.

Check for battery

If selected, indicates the system will check that a battery is properly connected and enable backup battery support.

Enable battery tests
If selected, indicates the panel will conduct both Low and High Loads test cycles on the attached battery to ensure it is usable.

Test time
Duration of battery test (Default is 10 seconds).

Low load test period
Interval between low load battery tests (Default is 3 minutes). The low load test is what is used to detect presence and state of the battery.

High load test period
Interval between high load battery tests (Do not run more than once every 20 hours as it may damage the battery).

Very low voltage (V)
Used by the system to detect when a battery is present.

Cutoff voltage (V)
This is the voltage where the battery is disconnected to prevent deep discharge and damage to the battery. This will send the “Backup Battery Critical” event and shut down the panel. Default is 10.2V. UL requires that the panel be able to operate down to 10.2V even though this is below what most battery vendors recommend. Default is 10.2V.

Warning voltage (V)
The voltage point at which the panel will send the Backup Battery Low event. The default voltage is 11.40V.

Low voltage (V)
When the “Low Battery Voltage” is reached, the system pseudo point reports low battery.

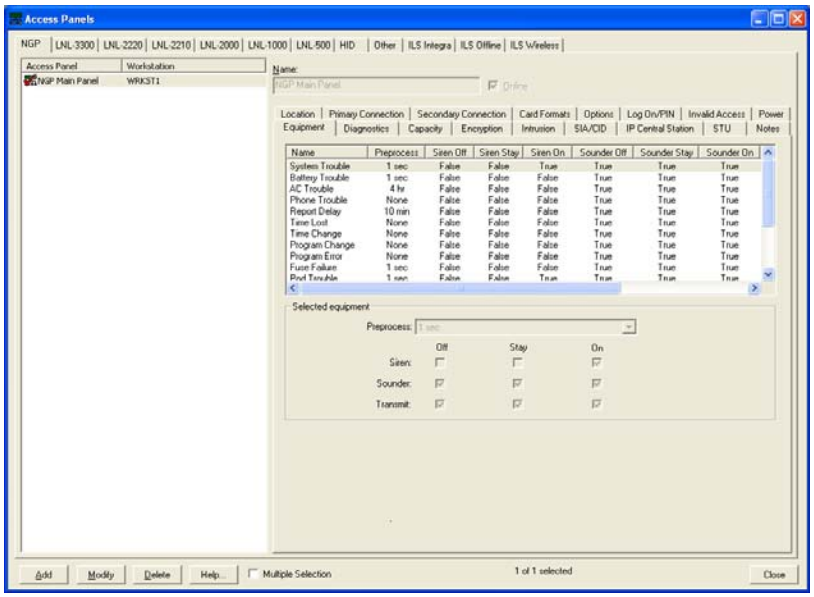
Excess charge voltage (V)
This is the voltage that will cause the battery to be cut off and the cut off time applied. Default 16.0V.

No current (mA)
This is the current that is used to determine if the battery is charging as opposed to being fully charged.

Excess power state discharge current (A)
When operating off of the battery and the current being supplied exceeds 1.2A this state is set at the keypad.

NGP Form (Equipment Sub-tab)

Equipment points allow an NGP access panel to report panel events into Alarm Monitoring. This screen allows you to configure the preprocess time and whether the event will be reported for each arming state.



Preprocess

The duration that the point must remain triggered before an alarm is audited.

Siren

Enable to cause the siren to sound for the selected alarm.

Sounder

Enable to cause the sounder to sound for the selected alarm.

Transmit

Enable to cause alarms to be transmitted for the selected alarm.

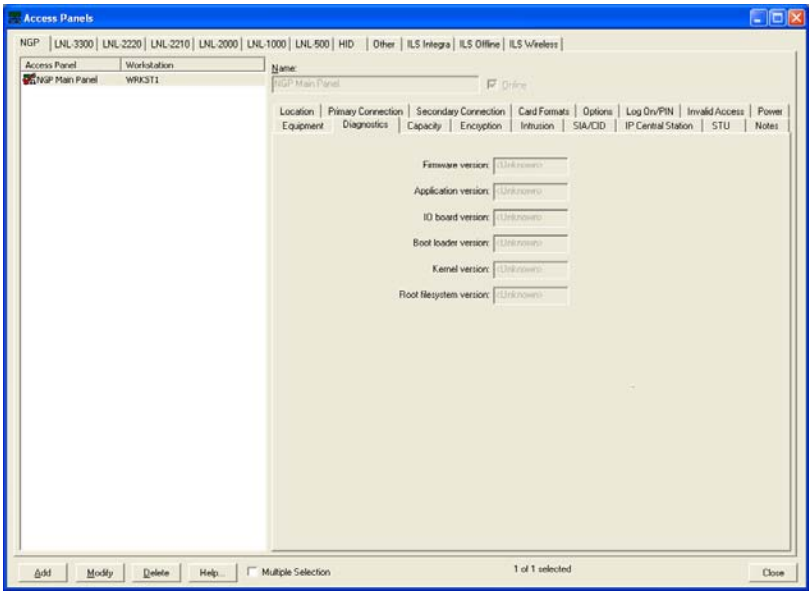
NGP Panel Equipment Point

Number	Name	Description
1	System Trouble	Main panel tamper only
2	Battery Trouble	Low and no battery conditions
3	AC Trouble	Loss of AC power
4	Phone Line Trouble	Loss of phone line voltage
5	Report Delay	Digital communications trouble
6	Time Lost	Main panel system time lost (warm boot)
7	Time Change	Main panel system time lost
8	Program Change	Main panel configuration altered

NGP Panel Equipment Point (Continued)

Number	Name	Description
9	Program Error	Error in main panel configuration. Errors can result from improper scheduling (e.g. two scheduled opens for an area which are back to back) or from configuring points which do not have a module group of points assigned to them.
10	Fuse Failure	Main panel fuse failure
11	Pod Trouble	Pod tamper, Pod SNAPP comms, Pod substitution
12	Pod Battery Low	Pod battery (probably only RF sensor batteries)
13	Pod Battery Change	Pod configuration altered
14	Pod Program Error	Error in Pod configuration
15	Misc Trouble (Future)	Miscellaneous trouble
16	HSC Trouble	High security comms trouble (MK 7), for HSC Pod

NGP Form (Diagnostics Sub-tab)



Firmware version

A read-only field that lists the firmware version of the panel. This is the firmware version of the package that is loaded to the panel and that will be displayed in Alarm Monitoring.

Application version

A read-only field that lists the application version of the panel.

IO board version

A read-only field that lists the IO board version of the panel.

Boot loader version

A read-only field that lists the boot load version of the panel.

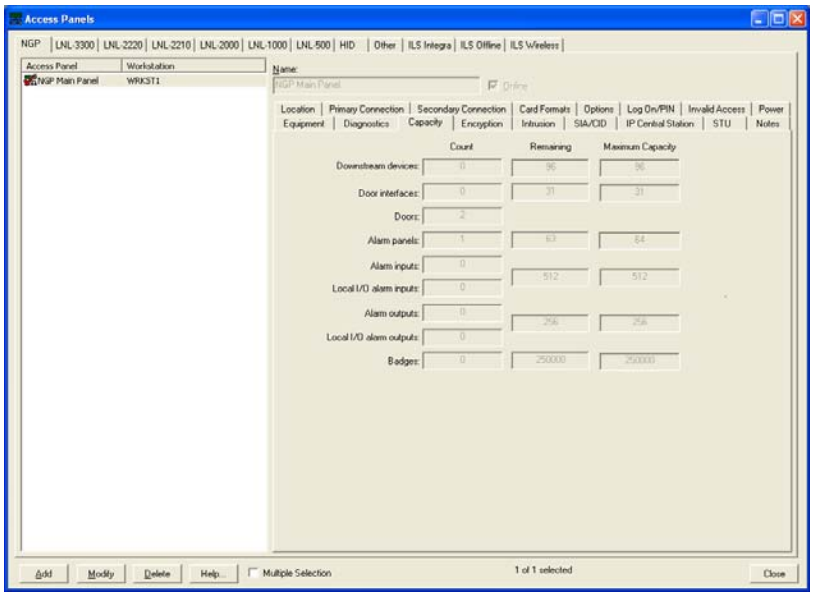
Kernel version

A read-only field that lists the kernel version of the panel.

Root filesystem version

A read-only field that lists the root filesystem version of the panel.

NGP Form (Capacity Sub-tab)



Doors

A read only field that list the number of doors currently being used, remaining that can be used, and the maximum allowed by the system.

Alarm panels

A read only field that list the number of alarm panels currently being used, remaining that can be used, and the maximum allowed by the system.

Alarm inputs

A read only field that list the number of alarm inputs currently being used, remaining that can be used, and the maximum allowed by the system.

Local I/O alarm inputs

A read only field that list the number of local I/O alarm inputs currently being used, remaining that can be used, and the maximum allowed by the system.

Alarm outputs

A read only field that list the number of alarm outputs currently being used, remaining that can be used, and the maximum allowed by the system.

Local I/O alarm outputs

A read only field that list the number of local I/O alarm outputs currently being used, remaining that can be used, and the maximum allowed by the system.

Downstream devices

A read only field that list the number of downstream devices currently being used, remaining that can be used, and the maximum allowed by the system.

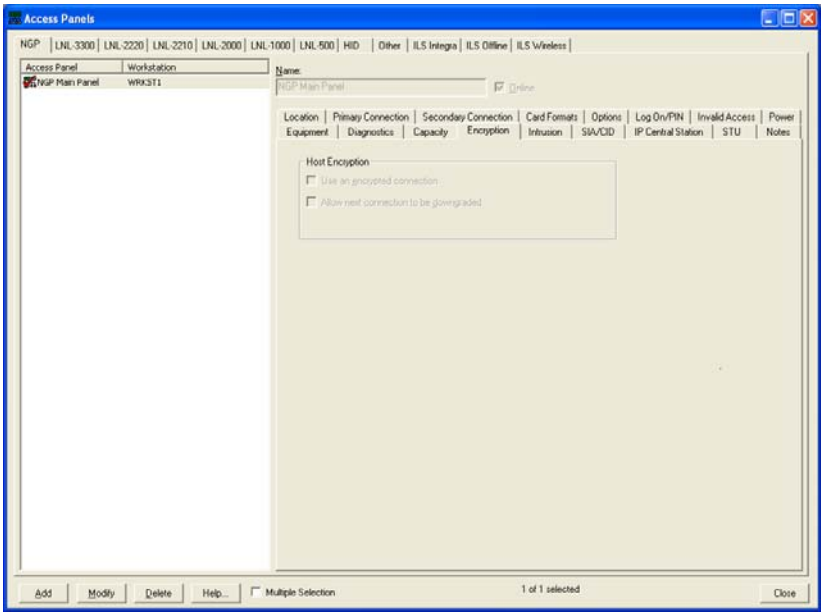
Door interfaces

A read only field that list the number of door interfaces currently being used, remaining that can be used, and the maximum allowed by the system.

Badges

A read only field that list the number of badges currently being used, remaining that can be used, and the maximum allowed by the system.

NGP Form (Encryption Sub-tab)



Use an encrypted connection

Enable to encrypt the connections used by the panel.

Allow next connection to be downgraded

Select this check box if you want the host/controller connection to downgrade the connection if the encryption connection fails. Displays only for manual key management systems.

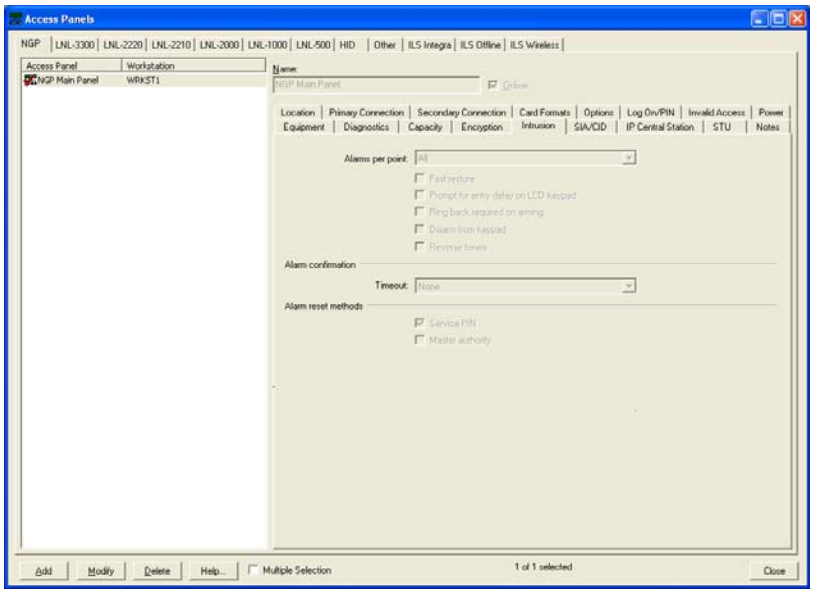
When this check box is selected, the access control system attempts the following connections (in sequence):

1. An encrypted connection with the inactive master key
2. An encrypted connection with the factory default value for Master Key 1
3. An encrypted connection with the factory default value for Master Key 2
4. A plain connection (only attempted if the controller does not require an encrypted connection)

If encryption is enabled the following connections are attempted in sequence:

1. An encrypted connection with the inactive master key.
2. A plain connection.

NGP Form (Intrusion Sub-tab)



Alarms per point

Set the number of consecutive alarms from an input point that the system will monitor. Any consecutive alarms will be ignored.

Fast restore

Enable to send a point restore within 1 minute. This is used rather than the Siren time field.

Prompt for entry delay on LCD keypad

Enable to ask a user via the keypad if they want the optional entry delay each time any area is set to “stay”. An entry delay provides time for an authorized entrant to disarm the area.

Ring back required on arming

Enable to cause a keypad tone and short siren squawk to confirm each time an area is armed. The Annunciate option on the LCD Keypad Areas Form on page 1554 must also enabled. Full

reporting mode on the area should also be selected. For more information, refer to Areas Form (Intrusion Detection Sub-tab) on page 760.

Disarm from keypad

Enable to allow an area to be disarmed from the keypad.

Reverse tones

Uses reverse tone signaling at the keypad.

Timeout

Select the length of time that must pass without action before the alarm confirmation times out. When **Timeout** is configured to any value other than "None" the system will confirm the alarm.

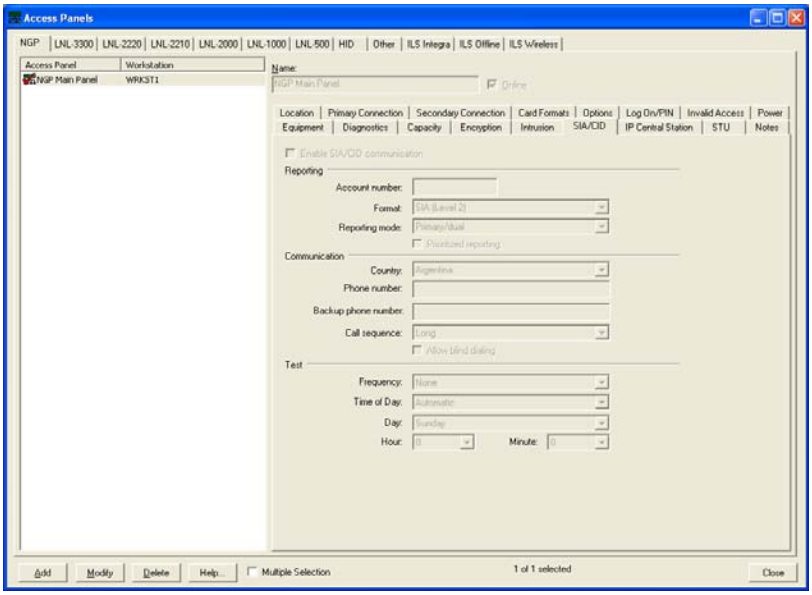
Alarm reset methods

Enable which method(s) can be used to reset a confirmed alarm. Choices include:

- Service PIN - indicates that a Service user must enter their ID and PIN on the keypad in order to reset the alarm. The Service user information is configured on the panel's Log On/PIN sub-tab. For more information, refer to NGP Form (Log on/PIN Sub-tab) on page 1534.
- Master authority - indicates that a Master authority user must enter their ID and PIN on the keypad in order to reset the alarm. Master authority is granted on the Access Levels > Permission Profiles sub-tab by enabling the **Master override** option. For more information, refer to Access Levels Form (Area Permissions (NGP) Sub-tab) on page 722.

IMPORTANT: You must disarm the area before confirmed alarms can be reset.

NGP Form (SIA/CID Sub-tab)



Enable SIA/CID communication

For NGP intrusion panels only. Select to enable SIA/CID communication.

IMPORTANT: The following limitations should be noted when SIA/CID communication is enabled and Contact ID is the format used for reporting alarms to Central Station:

- For NGP-2220i and NGP-3320i panels: If you configure more than 98 areas for the panel, all areas greater than 98 will report as “area 99” at the Central Station. Contact ID only supports two (2) digits for reporting the area information and the panel supports up to 150 areas.
- For NGP-3320i panels only: If you configure more than 512 inputs for the panel, all inputs greater than 512 will report as “input # 513” at the Central Station. Contact ID only supports three (3) digits for identifying a zone and the panel supports up to 1024 inputs.

Account number

This is the number used by the system to identify the panel.

Format

Select the format of the messages transmitted to the monitoring station.

Reporting mode

Select the mode of how the panel uses reporting through SID/CID.

Prioritized reporting

Enable to allow transmitting alarms in a prioritized manner instead of the order in which they occur.

Country

Identifies the country to control modem dialing rules.

Phone number

Enter the number the panel uses to transmit messages to the system.

Backup phone number

Enter the alternative number to be used if the primary number is unable to be used.

Call sequence

Set the call dialing sequence for the primary and backup phone numbers. The **Call Sequence** setting determines the number of attempts and delay period for transmitting alarms to the central station:

- ULC: PPBBPPBB / delay 60 minutes / PPBBPPBB / delay 60 minutes / PPBBPPBB / delay 60 minutes / PPBBPPBB
- UL: PPBBPPBBPB / delay 10 minutes
- Long: PPPPBBBB / delay 10 minutes / PPPPBBBB / delay 30 minutes / PPPPBBBB / delay 60 minutes / PPPPBBBB / delay 2 hours / PPPPBBBB
- FCC/ICAN: PPBP / delay 5 minutes / PPBP / delay 10 minutes / PPBP / delay 30 minutes / PPBP / delay 60 minutes / PPBP / delay 2 hours / PPBP

P = Primary phone number call attempt
B = Backup phone number call attempt

Note: After completing the sequence, the panel gives up trying to report the messages. The messages are lost. Any new message that becomes pending during the sequence will trigger the selected dial sequence again to start at the beginning.

Allow blind dialing

Select to enable blind dialing, which allows dialing whether or not a dial tone can be established.

Frequency

The length of time between (and time of occurrence for) automated SIA/CID test dialing of the reporting channels (HSC and/or dialer). This feature allows you to “stagger” the communications test times for multiple panels. For UL Listed systems: Communication testing must occur at least daily.

Time of Day

Select either “Automatic” or “Manual.” With “Automatic” selected, the test dialing time will be random, occurring sometime from 1:00 - 4:00 a.m.

Day

When **Time of Day** is Manual, select from “Sunday” - “Saturday.”

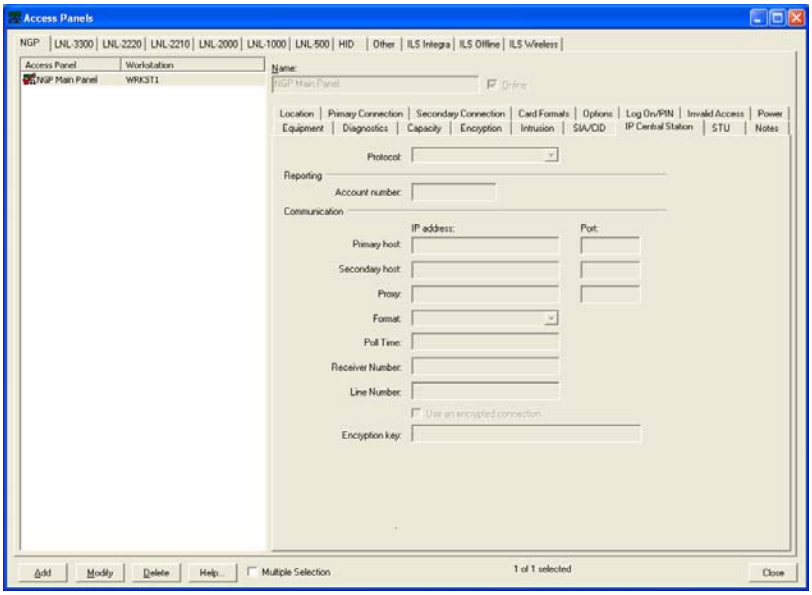
Hour

When **Time of Day** is Manual, select from 0 - 23 hours. “0” is the equivalent of midnight.

Minute

When **Time of Day** is Manual and **Frequency** is 12 hours, 1 day, or 1 week, select from 0 - 58 minutes.

NGP Form (IP Central Station)



Protocol

Select to enable HSC-IP, Osborne-Hoffman, or Bosch communication.

Account number

This is the number used by the receiver to identify the panel.

Primary host

Enter the primary host used to communicate with the system.

Port
Enter the port number for the primary host.

Secondary host
Enter the secondary host used to communicate with the system.

Port
Enter the port number for the secondary host.

Proxy
Enter the proxy address used to access the network.

Format
This is the alarm IP message format to be used.

- HSC-IP: SIA only
- Bosch: CID only
- Osborne-Hoffman: CID or SIA

Poll Time
For Osborne-Hoffman or Bosch receivers: Enter the how long after the last alarm message to send a poll (from 5 - 86400 seconds).

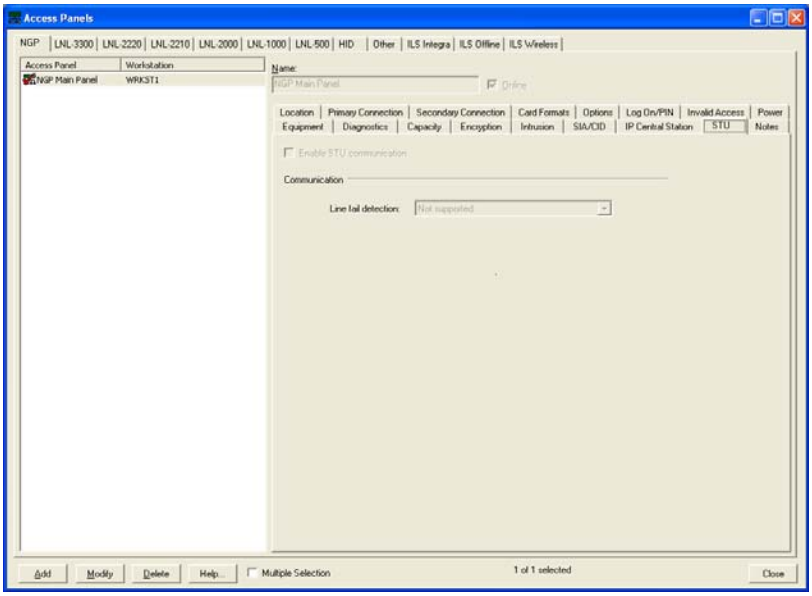
Receiver Number
For Osborne-Hoffman or Bosch receivers: This is the receiver gateway to which the alarm message is being sent. Enter a value from 1 - 9999.

Line Number
For Osborne-Hoffman or Bosch receivers: This is the line in the receiver gateway to which the alarm message is being sent. Enter a value from 1 - 9999.

Use an encrypted connection
For Bosch receivers only: Select this check box to enable an encrypted connection.

Encryption key
For Bosch protocol only: This is the AES key (32 hex bytes) for encrypting the communication to the alarm receiver.

NGP Form (STU Sub-tab)



Enable STU communication

Select to enable STU communication.

Line fail detection

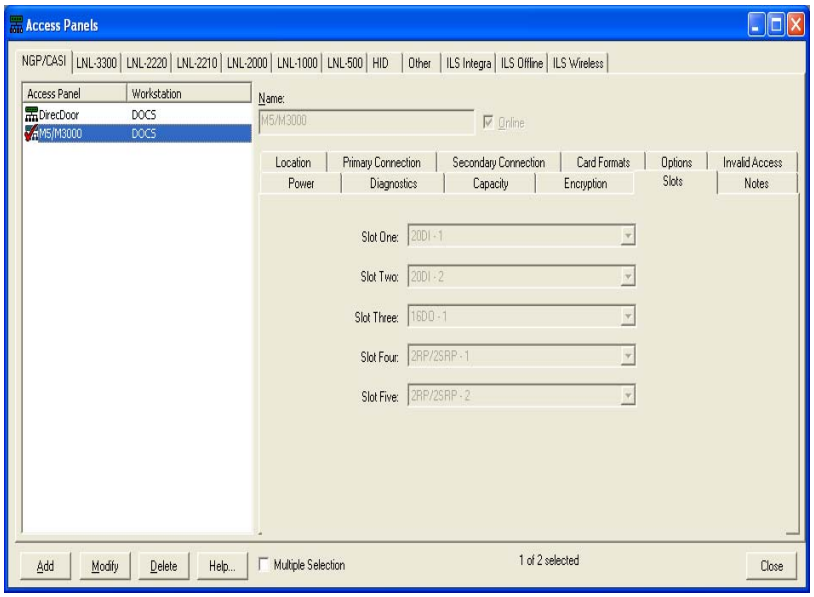
Enable to indicate if a line fail detection is supported and positive/negative polarity.N

NGP Form (Slots)

Available for DirecDoor and M5/M3000.

Use this form to assign up to five (5) device extension boards to the panel's slots.

IMPORTANT: Modifying access panel slot assignment will remove all devices associated with the changed slots.



Slot

DirecDoor: Select the "DDIO" board for **Slot One** to extend the number of DirecDoor devices. This allows you to configure up to four alarm panel inputs and four alarm panel outputs.

M5/M3000: All slots are available for slot assignment. Select a board for each slot as required to extend the number of M5/M3000 devices. Board types include:

- 2RP/2SRP-1, 2RP/2SRP-2, 2RP/2SRP-3, and 2RP/2SRP-4 boards which allow you to configure up to two additional readers each with one auxiliary output.
- 8RP-1 and 8RP-2 boards which allow you to configure up to eight additional readers.
- 20DI-1, 20DI-2, 20DI-3, and 20DI-4 boards which allow you to configure up to 20 additional alarm panel inputs.
- 16DO-1, 16DO-2, 16DO-3, and 16DO-4 boards which allow you to configure up to 16 additional alarm panel outputs.

Notes: M5/M3000 panels support up to two 8RP boards, four 2RP/2SRP boards, and four 20DI/16DO boards.

8RP boards cannot be mixed with 2RP or 2SRP boards.

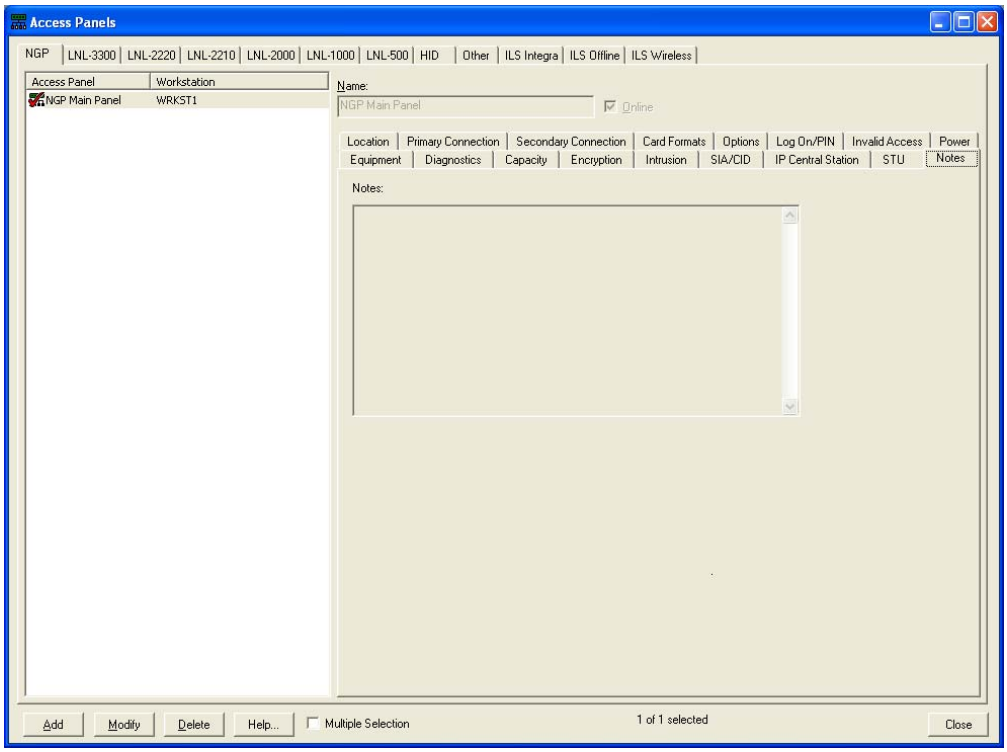
When you add a DirecDoor access panel, an onboard alarm panel is automatically assigned to it. Additional alarm panels may be automatically assigned depending on DirecDoor and M5/M3000 slot assignments.

Model	Alarm Panel	Maximum Inputs/Outputs
DirecDoor	DirecDoor Onboard	Supports up to 6 outputs
	DirecDoor DDIO	Supports up to 4 inputs and 4 outputs
M5/M3000	One M5/M3000 20DI per 20DI board	Supports up to 20 inputs
	One M5/M3000 16DO per 16DO board	Supports up to 16 outputs

When you add a DirecDoor access panel, an onboard alarm panel is automatically assigned to it.

Model	Alarm Panel	Maximum Inputs/Outputs
M2000	M2000 8DO	Supports up to 8 outputs
	M2000 10DI	Supports up to 10 inputs
	Note: Alarm panels are also automatically assigned when a M2000 panel is added but do not depend on slot assignment. For more information, refer to NGP Form (Options Sub-tab) on page 1532.	

NGP Form (Notes Sub-tab)



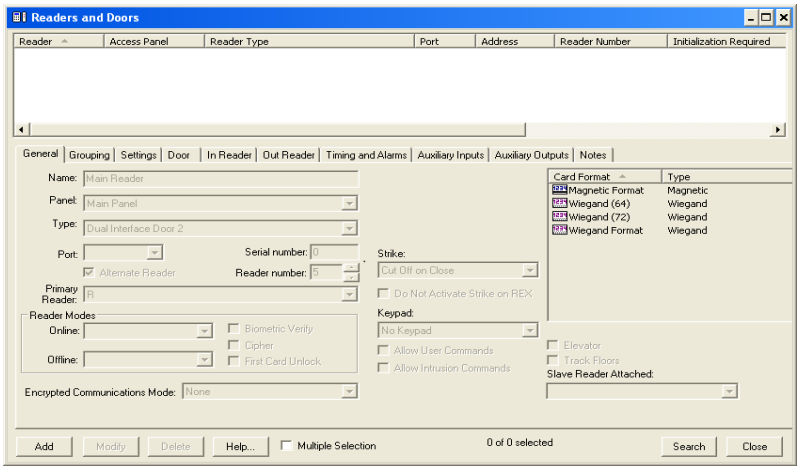
Notes

Enter information about the panel. This field is limited to less than 2000 characters. Any text that is entered here will be displayed in Alarm Monitoring. For more information, refer to the procedure to View Notes in the Alarm Monitoring User Guide, “Monitor Devices.”

NGP Readers Overview

The following reader forms are specific to NGP/CASI readers.

General Form



Listing window

Lists currently defined readers, the access panel to which each is connected, and each reader's type. It also lists the reader's port, address, and reader number.

Name

Enter a unique reader name of no more than 32 characters. The application uses the name when assigning card readers to access groups, when monitoring alarms, and elsewhere in the system.

Panel

Select the access panel to which the reader is attached. Choices include all currently defined access panels.

Type

Select the type of reader that is being configured. Available choices depend upon the type of access panel to which the reader is connected.

Notes: NGP reader types must be the same per door. Each NGP door controller supports both IN (entry) and OUT (egress) readers. The reader technology, Wiegand or magnetic, must be the same for both readers.

Note: Keypads and readers with keypads assigned to NGP baseboards or CASI controllers with 2RP or S2RP boards support Wiegand data, only.

Serial number

Also known as the host address. Enter the serial number of the specific reader. This allows the software to identify each panel. The serial number is typically hand-written (5 digits) on a small sticker on the circuit board. This field is available for off-board reader types. For on-board reader types, the doors will automatically get a serial number.

Reader number

For CASI doors only: Identifies the reader. The reader number must be unique for each reader and conform to the configurations supported by the panel model.

- DirecDoor: Reader numbers 1-2 are available:
  - 1 reader with 2 doors

  - 2 readers with 1 door
- M2000: Reader numbers 1-4 are available:
  - 4 doors (1 reader per door)
  - 3 doors (2 readers + 1 reader + 1 reader)
  - 2 doors (2 readers per door)
- M5/M3000: Reader numbers 1-8 or 1-16 are available depending on which device extension boards are present. 2RP/2SRP boards support up to 8 doors and 8RP boards support up to 16 doors.

Allow User Commands

Select this check box if you are configuring a command reader. A *command reader* is equipped with a keypad by which system functions are performed.

Note: This check box must be selected before you specify the actions triggered by the keypad entries. Actions are specified using the Command Programming form of this folder.

Strike

Indicates how the door strike behaves when a valid card swipe occurs. Choices include:

- **Cut off on Close** – cuts off the door strike when the door closes. This is the default setting.
- **Cut off on Open** – cuts off the door strike when the door opens.
- **Cut off on Duration** - cuts off the door strike when the strike time expires. **Strike time** is configured on the Timing and Alarms form. For more information, refer to Timing and Alarms Form on page 1564.

Note: Available for NGP Universal Door Controllers. However, support for the legacy door controllers (NGP-1300 and NGP-1320) is limited to “Cut off on Close” only.

Card Format

Lists the format(s) expected when a card is presented to the reader. Card formats are defined in the Card Formats folder.

Note: Card formats for NGP/CASI and HID readers are automatically specified based on the card formats selected for the access panel to which the reader is assigned and cannot be modified on the General form. For more information, refer to the NGP Form (Card Formats Sub-tab) on page 1531 and HID Form (Card Formats Sub-tab) on page 624.

Add

Adds a reader to the system.

Modify

Changes a reader entry.

Delete

Removes the selected reader(s).

Help

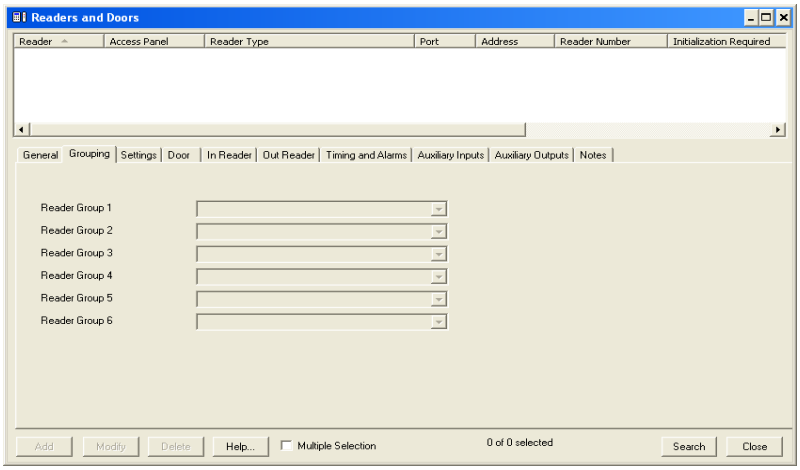
Displays pertinent help information onscreen.

Multiple Selection

If selected, two or more reader entries can be simultaneously checked in the listing window.

Close
Closes the Readers folder.

Grouping Form



Listing window
Lists currently defined readers (locks), the controller panel to which each is connected, and each lock's type. It also lists the lock's ID (Reader number).

Reader Groups
Specify groups for the selected reader (lock) from the Reader Group drop-down lists. Choices include the reader (lock) group values that were added in the List Builder folder.

Search
Displayed in view mode on every form in the Readers folder. This button is used to search for and list existing readers (locks) that meet the specified lock group search criteria.

Modify
Allows you to change reader (lock) group entries.

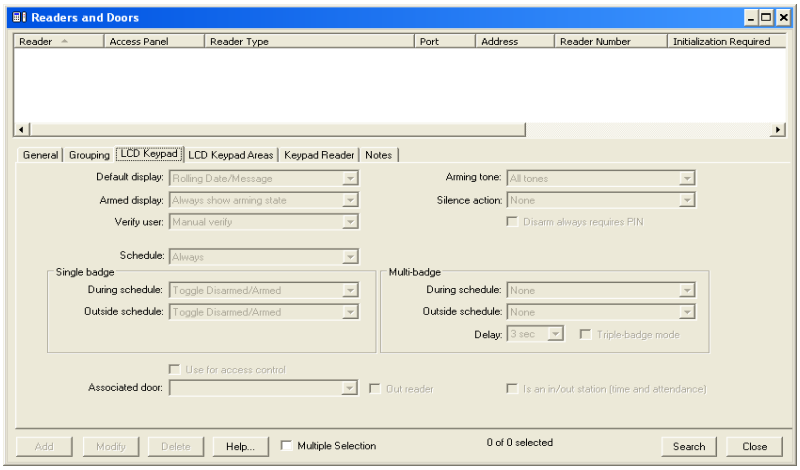
Help
Displays pertinent help information.

Multiple Selection
If selected, two or more reader (lock) entries can be simultaneously selected in the listing window.

Close
Closes the Readers folder.

LCD Keypad Form

This screen only appears if the reader type is an LCD keypad.



Listing window

Lists currently defined readers (locks), the controller panel to which each is connected, and each lock's type. It also lists the lock's ID (Reader number).

Default display

Select what is displayed on the keypad display screen.

Armed display

Select what is displayed on the keypad display screen when in an armed state.

Verify user

Select how a user is verified (by entering their PIN) after silencing an alarm.

Arming tone

Select whether the entry and exits tones will sound.

Silence action

Allows setting the keypad to auto-silence and/or have all of the user's authorized areas disarm automatically when someone logs into this keypad.

Disarm always requires PIN

Enable to always require a user to enter their PIN when disarming an area.

Schedule

Select the schedule that the display and tone settings will be active.

Single badge

Select the in and out of schedule options for a single credential holders.

Multi-badge

Select the in and out of schedule options for multiple credential holders.

Delay

For multi-badge, select the delay needed between presenting multiple credentials.

Triple-badge mode

For multi-badge, enable to require triple-badging.

Use for access control

Enable to use the reader/door for access control.

Associated door

Select the associated reader/door to be used for access control.

Out reader

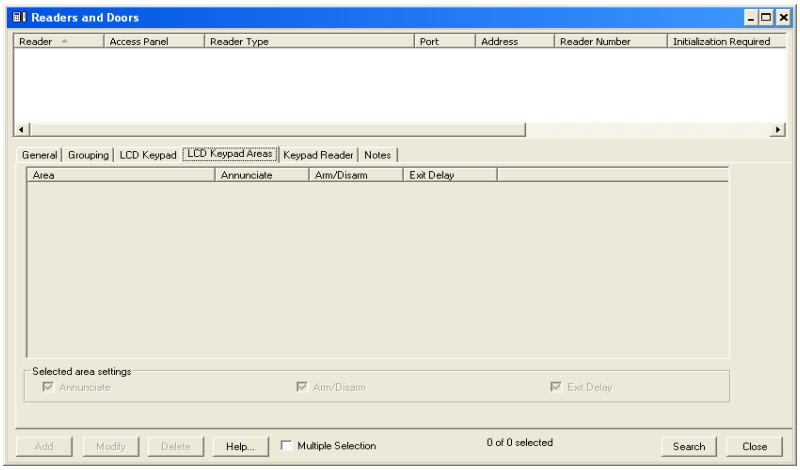
Enable if the associated reader/door is an out reader.

Is an in/out station (time and attendance)

Enable to have the reader/door be used to log cardholder arrivals and departures.

LCD Keypad Areas Form

This screen only appears if the reader type is an LCD keypad.



Listing window

Lists currently defined readers (locks), the controller panel to which each is connected, and each lock's type. It also lists the lock's ID (Reader number).

Area listing window

Select the area(s) that the selected area settings will affect.

Annunciate

Enable to have the keypad signal when it is arming.

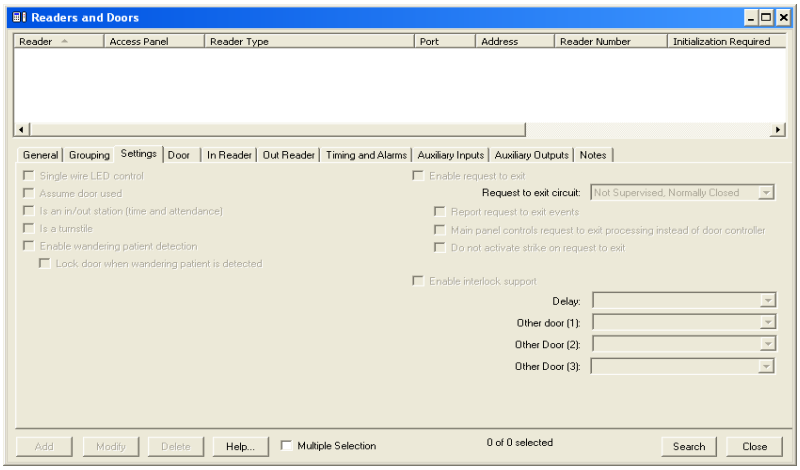
Arm/Disarm

Enable to allow cardholders to arm and disarm an area.

Exit Delay

Enable to allow a brief exit delay to allow cardholders to leave the area selected.

Settings Form



Single wire LED control

If selected, LED control will be via a single wire. Use the RED LED connector on the reader port. Not available for CASI readers.

Assume door used

Select to enable the detection of a user entering using the selected reader.

Is an in/out station (time and attendance)

Select if the reader being used is to log cardholder arrivals and departures.

Note: This option must be enabled (selected) in order to include records on the Cardholder Time and Attendance report.

Is a turnstile

Select if the reader being used is a turnstile that is being used with antipassback and escort-required users.

Enable wandering patient detection

Select to enable detection of wandering patients.

Lock door when wandering patient is detected

Select to cause the door to lock when a wandering patient is detected.

Enable request to exit

Select to enable a REX request.

If selected for CASI readers, **Do not activate strike on request to exit** will be enabled.

Request to exit circuit

Select the circuit type used for the REX wiring on the door. You can configure up to eight (8) different circuit types (EOL resistor tables) *per* panel.

Report request to exit events

Select to send reports on request to exit events.

Main panel controls request to exit processing instead of door controller

Select if you want the main panel to control all REX requests instead of the door controller. Not available for CASI readers.

Do not activate strike on request to exit

A REX (Request to Exit) contact is typically a button located near the associated door. When a cardholder pushes the button a REX is sent to the panel. If this check box is selected, the door strike will NOT energize when the REX contact closes. If this check box is not selected, the door strike energizes when the REX closes.

Enable interlock support

Select to allow this door to be interlocked with up to 3 doors (defined in the Other door (#) fields) attached to the same access panel. An interlocked door cannot be opened unless the other doors selected are NOT opened.

Delay

Used with Reader interlock. All users will be denied access to this door until all other interlocked doors (up to 3) have been closed (and re-locked) for the selected “Delay” time-period.

Other door (1)

Used in conjunction with the Enable interlock support field. Select a door to interlock with another door. All doors that are interlocked must be attached to the same NGP access panel.

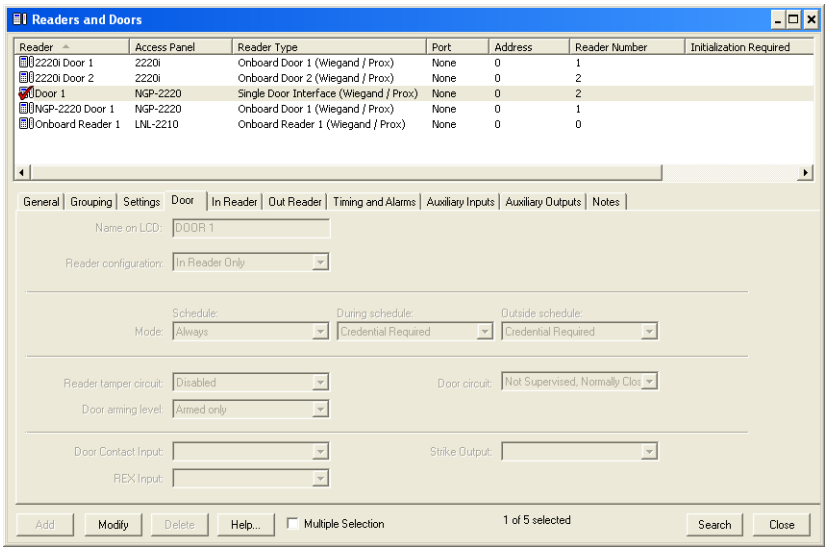
Other door (2)

Used in conjunction with the Enable interlock support field. Select a door to interlock with another door. All doors that are interlocked must be attached to the same NGP access panel.

Other door (3)

Used in conjunction with the Enable interlock support field. Select a door to interlock with another door. All doors that are interlocked must be attached to the same NGP access panel.

Door Form



Name on LCD

Enter the name that will appear on the LCD keypad. Not available for CASI panels.

Reader configuration

Select if your system is using in readers or in and out readers.

Notes: If you change **Reader Configuration** from “In and Out Readers” to “In Reader Only” and Out Reader is set in Door Contact, Rex or Strike, the system will automatically change this setting to “In Reader.”

“In and Out Readers” must be selected in order to include records on the Cardholder Time and Attendance report.

Mode

Set the door mode including:

- **Schedule** - Select the schedule (timezone) for the door mode. During the time interval specified for the timezone, the door will unlock based on the selected mode. For more information, refer to Timezones Form on page 708.
- **During schedule** - Select one of the following modes for when the schedule is enabled:
  - **Credential Required** - Unlocks the door when a valid user is granted access, and then locks the door after the strike time expires. Valid users are cardholders authorized to access the area at the scheduled time.
  - **Unlocked** - Unconditionally unlocks the door ignoring the arming state of the area associated with the door.
  - **Pending First User** - In this mode, the door remains in a locked state until the first valid user is granted access to the door. Once a valid user is granted access, the door will unlock and remain unlocked until the door mode changes based on schedule transitions.
  - **Unlocked if Disarmed** - Unlocks the door only if the area on either side of the door is Disarmed.
  - **Unlocked if Stay or Disarmed** - Unlocks the door only if the area on either side of the door is Stay or Disarmed.
- **Outside schedule** - Select one of the following modes for when the schedule is disabled:
  - **Credential Required** - Unlocks the door when a valid user is granted access, and then locks the door after the strike time expires. Valid users are cardholders authorized to access the area at the scheduled time.
  - **Unlocked** - Unconditionally unlocks the door ignoring the arming state of the area associated with the door.
  - **Pending First User** - In this mode, the door remains in a locked state until the first valid user is granted access to the door. Once a valid user is granted access, the door will unlock and remain unlocked until the door mode changes based on schedule transitions.
  - **Unlocked if Disarmed** - Unlocks the door only if the area on either side of the door is Disarmed.
  - **Unlocked if Stay or Disarmed** - Unlocks the door only if the area on either side of the door is Stay or Disarmed.

Reader tamper circuit

Select the wiring type used with the reader tamper circuit of the door. Choices include:

- **Not Required**: Disables the reader tamper input.
- **Converted TDC/PDC Door Controllers**: These units do not support dedicated/separate reader tamper monitoring.

Door circuit

Select the wiring type used with the door contact of the door. You can configure up to eight (8) different wiring types (EOL resistor tables) per panel.

Door arming level

Select the area arming levels for which the door is to be monitored.

Door Contact Input

For CASI doors only: Select the input to be used with the reader door contact of the door.

Possible options include: In Reader door contacts, Out Reader door contacts, alarm panels, and 20 DI alarm inputs.

Notes: Each reader has two dedicated inputs that can be used as a Door Contact and REX, and one dedicated output that can be used as Strike.

Out Reader door contact is available if an Out Reader is configured.

REX Input

For CASI doors only: Select the input to be used with the reader REX input of the door.

Possible options include: In Reader REX, Out Reader REX, alarm panels, and 20 DI alarm inputs.

Note: Out Reader REX is available if an Out Reader is configured.

Strike Output

For CASI doors only: Select the output to be used with the reader strike output of the door.

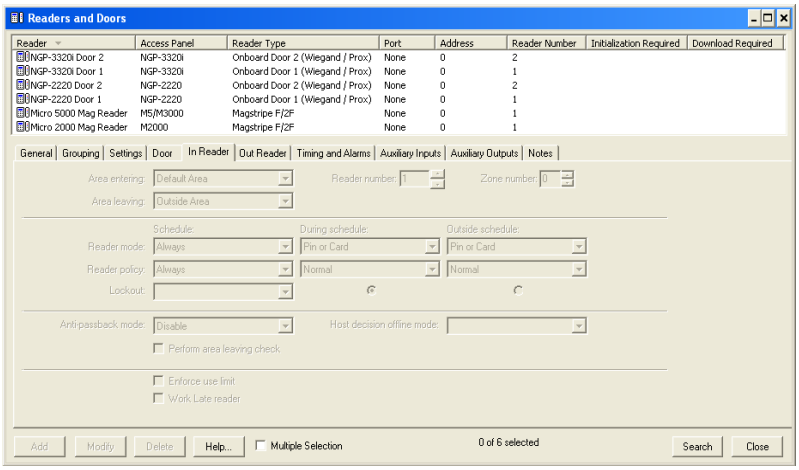
Possible options include: In Reader Strike, Out Reader Strike, In Reader auxiliary outputs, Out Reader auxiliary outputs, alarm panels, and 16 DO alarm outputs.

Notes: Each reader has one dedicated output that can be used as Strike output. In addition, 2RP/SRP-based readers have one auxiliary output that can be configured as Auxiliary Output or Door Strike.

In Reader auxiliary output and Out Reader auxiliary output are available for 2RP/2SRP-based readers only.

Out Reader Strike and Out Reader auxiliary output are available if an Out Reader is configured.

In Reader Form



Note: NGP/CASI reader types must be the same per door. Each NGP/CASI door controller supports both IN (entry) and OUT (egress) readers. The reader technology, Wiegand or magnetic, must be the same for both readers.

Area entering

Identifies the area a cardholder enters by using this reader. This area will be used for both intrusion reporting and anti-passback. Area anti-passback prevents a cardholder from gaining access to an area without first using his/her card to move out of the area.

Available areas are those defined on the Anti-Passback Areas form of the Areas folder.

Area leaving

Identifies the area a cardholder exits by using this reader. This area will be used for both intrusion reporting and anti-passback. If a cardholder attempts to enter an area he/she is already in, an APB violation will be noted.

Available areas are those defined on the Anti-Passback Areas form of the Areas folder.

Reader number

For CASI doors only: Identifies the IN (entry) reader. The IN reader number is configured when you add the reader on the General form.

Zone number

For doors assigned to NGP intrusion panels (NGP-2220i and NGP-3320i).

Identifies the Central Station reporting zone for the area that this point is associated with. Enter a value from 0 - 998. The default value is zero (0). All zone numbers except the default value must be unique within a given area.

Reader mode

Select the schedule that will control the reader and select the MODE (Card only, Card and Pin, Pin or Card, Pin Only) that will be active during and outside the schedule.

Note: Magnetic keypad devices (including readers with keypads) assigned to NGP baseboards or CASI controllers with 2RP or S2RP boards do not support pin reader modes. These devices support Wiegand data, only.

Reader policy

Select the schedule that will control the reader and select the POLICY (Normal, Dual Custody, Escort, Toggle Lock: All Users, Toggle Lock Authorized Users) that will be active during and outside the schedule.

Lockout

Signifies if the reader is disabled. Select the different schedule settings for this mode from each of the drop-down boxes.

Anti-passback mode

Select the level of anti-passback setting for this reader.

Host decision offline mode

This option is used for Global Anti-Passback to inform the panel what to do in case the panel is offline from the host. For this option to be available, you must:

- Have Global Anti-Passback enabled. On non-segmented systems, this is done by selecting the **Global Anti-Passback** check box on the Anti-Passback form in the System Options folder. On segmented systems, this check box is available on the Anti-Passback sub-tab of the Segments form in the Segments folder.

On this form:

- Verify the **Area entering**.
- Select "Hard APB" as the **Anti-passback mode**. If "Soft APB" is selected, APB is not enforced.

For Global Anti-Passback, the panel requests a decision from the host to determine if the cardholder will be allowed access to the reader. When the panel is offline from the host this request cannot be performed, so the panel will allow access based on this setting. Choices include:

- Deny all access attempts - All access attempts at this reader when the panel is offline with the host will be denied.
- Make local decision at panel - All access attempts at this reader when the panel is offline will be granted access based on the local settings in the panel (proper access level, etc.).

Perform area leaving check

If selected, the area leaving will be evaluated. Based on the **Area entering** and **Area leaving** selections for the reader, the system determines which area is to be associated with events for this device. This determination is made using the following rules:

- At least one area MUST be Local to the panel (not an Outside or a Global Area), and this Local Area will be used for intrusion reporting.
- If BOTH areas of the reader are Local to the panel, then the **Area entering** is used for intrusion reporting.

IMPORTANT: When Global Anti-passback is enabled at least one area must be Local to the panel in order to use the Local Area for intrusion reporting.

Enforce use limit

If this check box is selected, badge use limits are enforced at this reader. This means that each time a use-limited badge is used at this reader, the badge's use limit is decremented for the associated access panel. A cardholder's use limit is specified on the Badge form of the Cardholders folder.

Whenever the cardholder swipes his badge at a reader where use limits are enforced, the cardholder's use limit is reduced by one (1). When the use count reaches zero (0), the cardholder is unable to access use limit-enforced card readers on that panel.

A cardholder's use limit stays in effect until someone manually resets it from within Alarm Monitoring (by right-clicking on the entry for the use limit exceeded alarm) or by manually executing or scheduling a reset use limit action (For more information, refer to Reset Use Limit Properties Window on page 1248.). It should be noted that if a full database download is performed the use limit is preserved.

Some applications of the Use Limit:

- for use by temporary employees or visitors
- for use at readers that control access to commissaries or other locations of supplies, equipment, or provisions. With use limits enforced in these areas, the cardholder's badge functions like a debit card.

Work Late reader

For doors assigned to NGP intrusion panels (NGP-2220i and NGP-3320i).

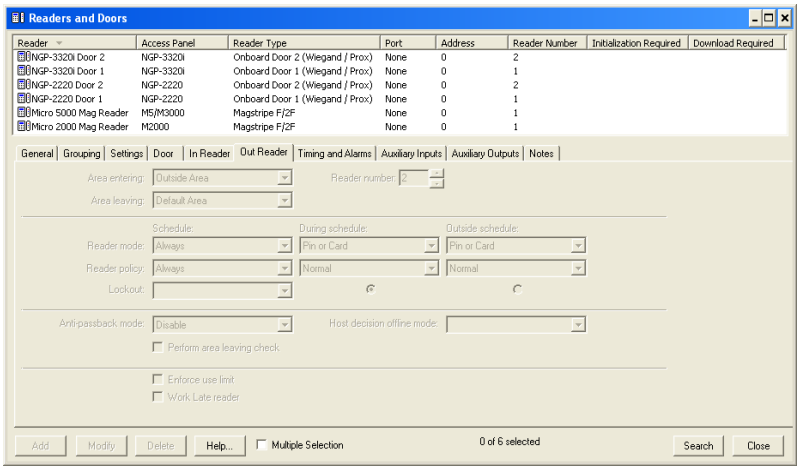
If selected, the Work Late feature is available at this reader. That means each time a badge with work late privileges is presented to this reader and granted access, the area's scheduled closing time will be delayed for a specified delay interval.

The Work Late condition can only be activated within 15 minutes prior to area arming. However the user can activate this condition prior to the 15 minutes interval using the keypad.

Scheduled closing time delay: Select the delay interval from the Areas > Arming/Disarming sub-tab > **Work late input** drop-down.

Work late permission: If granted, the user is allowed to extend the scheduled closing time. For more information, refer to Configure Permission Profiles on page 1576.

Out Reader Form



Note: NGP/CASI reader types must be the same per door. Each NGP/CASI door controller supports both IN (entry) and OUT (egress) readers. The reader technology, Wiegand or magnetic, must be the same for both readers.

Area Entering

Identifies the area a cardholder enters by using this reader. This area will be used for both intrusion reporting and anti-passback. Area anti-passback prevents a cardholder from gaining access to an area without first using his/her card to move out of the area.

Available areas are those defined on the Anti-Passback Areas form of the Areas folder.

Note: When the IN reader is configured, the OUT reader **Area entering** is automatically configured in reverse. The IN reader **Area leaving** is used for OUT reader **Area entering**.

Area leaving

Identifies the area a cardholder exits by using this reader. This area will be used for both intrusion and anti-passback. If a cardholder attempts to enter an area he/she is already in, an APB violation will be noted.

Available areas are those defined on the Anti-Passback Areas form of the Areas folder.

Note: When the IN reader is configured, the OUT reader **Area leaving** is automatically configured in reverse. The IN reader **Area entering** is used for the OUT reader **Area leaving**.

Reader number

For CASI doors only: Identifies the OUT reader. The reader number must be unique for each OUT reader. Based on availability, valid reader numbers include:

- DirecDoor: 1-2
- M2000: 1-4
- M5/M3000: 1 - 16

Reader mode

Select the schedule that will control the reader and select the MODE (Card only, Card and Pin, Pin or Card, Pin Only) that will be active during and outside the schedule.

Note: Magnetic keypad devices (including readers with keypads) assigned to NGP/CASI controllers do not support pin reader modes.

Reader policy

Select the schedule that will control the reader and select the POLICY (Normal, Dual Custody, Escort, Toggle Lock: All Users, Toggle Lock Authorized Users) that will be active during and outside the schedule.

Lockout

Signifies if the reader is disabled. Select the different schedule settings for this mode from each of the drop-down boxes.

Anti-passback mode

Select the level of anti-passback setting for this reader.

Host decision offline mode

This option is used for Global Anti-Passback to inform the panel what to do in case the panel is offline from the host. For this option to be available, you must:

- Have Global Anti-Passback enabled. On non-segmented systems, this is done by selecting the **Global Anti-Passback** check box on the Anti-Passback form in the System Options folder. On segmented systems, this check box is available on the Anti-Passback sub-tab of the Segments form in the Segments folder.
- Verify the **Area entering**.

- Select “Hard APB” as the **Anti-passback mode**. If “Soft APB” is selected, APB is not enforced.

For Global Anti-Passback, the panel requests a decision from the host to determine if the cardholder will be allowed access to the reader. When the panel is offline from the host this request cannot be performed, so the panel will allow access based on this setting. Choices include:

- Deny all access attempts - All access attempts at this reader when the panel is offline with the host will be denied.
- Make local decision at panel - All access attempts at this reader when the panel is offline will be granted access based on the local settings in the panel (proper access level, etc.).

Perform area leaving check

If selected, the area leaving will be evaluated. Based on the **Area entering** and **Area leaving** selections for the reader, the system determines which area is to be associated with events for this device. This determination is made using the following rules:

- At least one area MUST be Local to the panel (not an Outside or a Global Area), and this Local Area will be used for intrusion reporting.
- If BOTH areas of the reader are Local to the panel, then the **Area entering** is used for intrusion reporting.

IMPORTANT: When Global Anti-passback is enabled at least one area must be Local to the panel in order to use the Local Area for intrusion reporting.

Enforce use limit

If this check box is selected, badge use limits are enforced at this reader. This means that each time a use-limited badge is used at this reader, the badge’s use limit is decremented for the associated access panel. A cardholder’s use limit is specified on the Badge form of the Cardholders folder.

Whenever the cardholder swipes his badge at a reader where use limits are enforced, the cardholder’s use limit is reduced by one (1). When the use count reaches zero (0), the cardholder is unable to access use limit-enforced card readers on that panel.

A cardholder’s use limit stays in effect until someone manually resets it from within Alarm Monitoring (by right-clicking on the entry for the use limit exceeded alarm) or by manually executing or scheduling a reset use limit action (For more information, refer to Reset Use Limit Properties Window on page 1248.). It should be noted that if a full database download is performed the use limit is preserved.

Some applications of the Use Limit:

- for use by temporary employees or visitors
- for use at readers that control access to commissaries or other locations of supplies, equipment, or provisions. With use limits enforced in these areas, the cardholder’s badge functions like a debit card.

Work Late reader

For doors assigned to NGP intrusion panels (NGP-2220i and NGP-3320i).

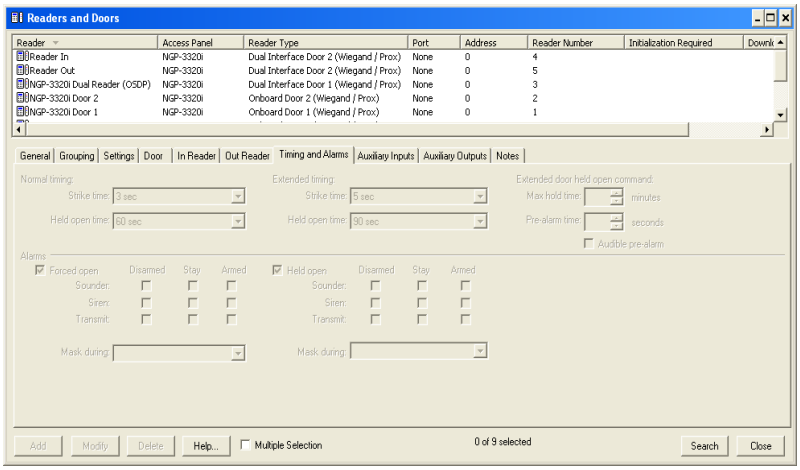
If selected, the Work Late feature is available at this reader. That means each time a badge with work late privileges is presented to this reader and granted access, the area’s scheduled closing time will be delayed for a specified delay interval.

The Work Late condition can only be activated within 15 minutes prior to area arming. However the user can activate this condition prior to the 15 minutes interval using the keypad.

Scheduled closing time delay: Select the delay interval from the Areas > Arming/Disarming sub-tab > **Work late input** drop-down.

Work late permission: If granted, the user is allowed to extend the scheduled closing time. For more information, refer to Configure Permission Profiles on page 1576.

Timing and Alarms Form



Normal timing

Select the series of alarm options for when a door is held open. The options are the same for when a door is forced open.

Extended timing

Select the series of alarm options for when a door is forced open. The options are the same for when a door is held open.

Extended door held open command

Select the series of alarm options for when a door is considered held open for an extended amount of time.

Forced open

Select to allow alarms when a door is forced open. Not available for CASI readers.

Sounder

Select to enable the sounder when a door is forced open.

Siren

Select to enable the siren when a door is forced open.

Transmit

Select to enable alarms to be transmitted when a door is forced open.

Mask during

Select when a forced open alarm is masked.

Held open
Select to allow alarms when a door is held open. Not available for CASI readers.

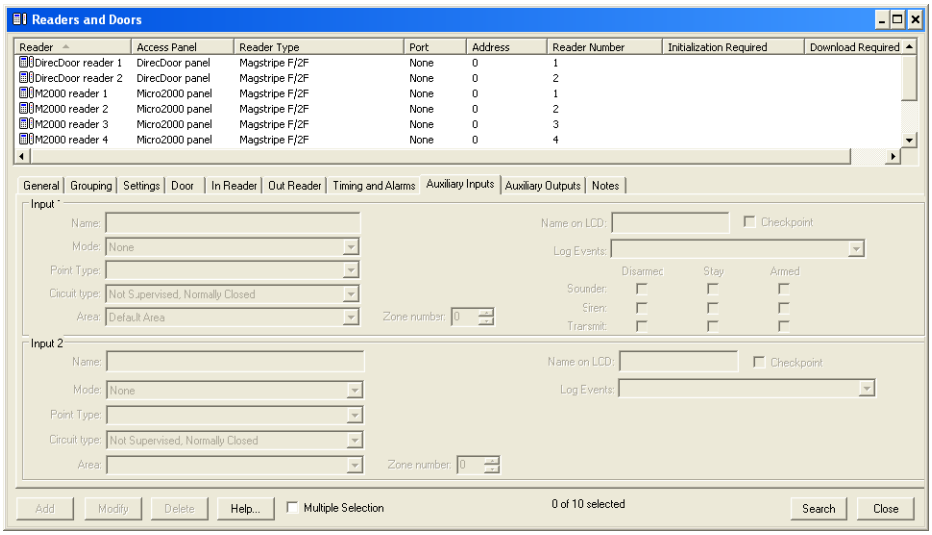
Sounder
Select to enable the sounder when a door is held open.

Siren
Select to enable the siren when a door is held open.

Transmit
Select to enable alarms to be transmitted when a door is held open.

Mask during
Select when a held open alarm is masked.

Auxiliary Inputs Form



Note: CASI panels do not support auxiliary inputs.

Name
Enter a name for the reader auxiliary input. The name you use will display in Alarm Monitoring.

Mode
Select the auxiliary input mode. This specifies how the auxiliary input relay on the door-controller module is to be used.

- **Magnetic lock bond sense** - Specifies that the input is to be used for a simple lock bond sensor or latch-keeper detection. Enables the output from the lock bond sensor to be monitored. Ensures that the magnetic lock is secured within five (5) seconds. The bond sensor alarm can be configured based on area armed state.
- **Extended request to exit** - Used in conjunction with the “Door opener” auxiliary output mode to delay the strike. Triggers the automatic door opener if **Extended strike/held times** is specified for the cardholder.

Point Type

Select the type of sensor and/or the type of monitoring to be used with this point. Specifies an input point on the perimeter of an area. Available selections include many pre-defined types plus custom types 80-99 that can be set up manually. For more information, refer to Input Point-Type Reference on page 1578.

Notes: Readers assigned to NGP non-intrusion panels are pre-configured to “Standard.”

Circuit type

Select the auxiliary input circuit type. You can configure up to eight (8) different wiring types (EOL resistor tables) *per* panel.

Area

The area that this point is associated with.

Zone number

For inputs associated with NGP intrusion panels (2220i and 3320i). Identifies the Central Station reporting zone for the area associated with this point. Enter a value from 0 - 998. The default value is zero (0). All zone numbers except the default value must be unique within a given area.

Name on LCD

The name as it will appear on the LCD keypad.

Checkpoint

Select this check box to designate the device as a checkpoint. This device will be listed along with all other devices that have this check box selected when the **Only show devices marked as checkpoints** check box is selected when adding a guard tour.

Log Events

Select the timezone during which events originating at this alarm input are to be logged by the system. If this field is left blank, all events from this input will be recorded.

Sounder

Select to enable the sounder on the keypad to sound for the magnetic lock.

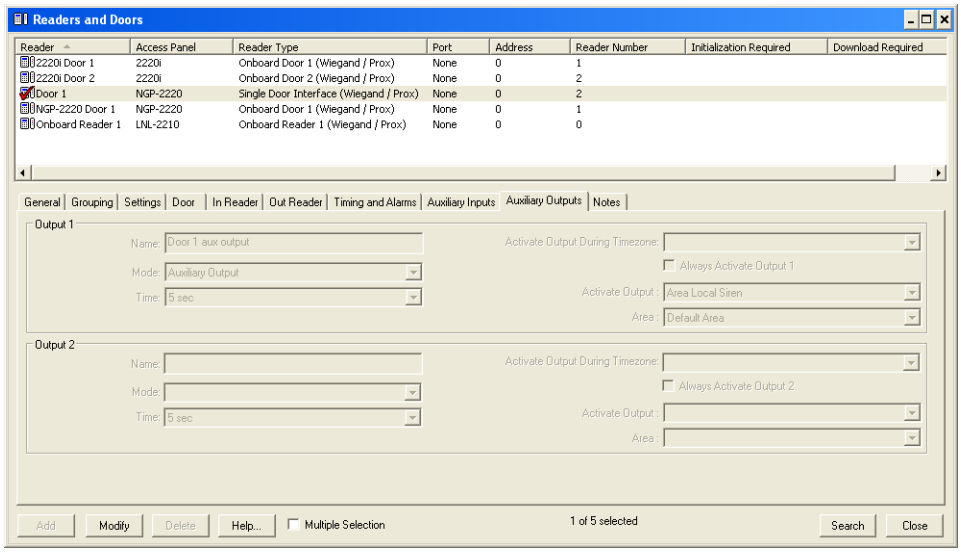
Siren

Select to enable the siren to sound for the magnetic lock.

Transmit

Select to enable transmission to central station for the magnetic lock.

Auxiliary Outputs Form



Note: Available for M5/M3000 2RP/2SRP reader modules only. Each 2RP/2SRP module has one (1) auxiliary output. Outputs #1 and #2 are available if “In and Out Readers” is configured for the door controller.

Name

Enter a name for the reader auxiliary output. The name you use will display in Alarm Monitoring.

Mode

Select the reader auxiliary output mode. This specifies how the auxiliary output relay on the door-controller module is to be used.

For NGP readers, choices include:

- **Activate on door held or forced open** - Enables the output to activate whenever a Door Forced Open or Door Held Open alarm is detected.
- **Door opener** - Enables a push paddle contact to operate the door opener on the secure side of the door. Utilizes the extended strike/held open times for the door.

Note: **Extended request to exit** must be selected as the auxiliary input mode. Badges configured to **Use extended strike/held times** will also activate the door opener.

For CASI M5/M3000 readers: Select “Auxiliary Output” to specify that the 2RP/2SRP module is to be used as a general purpose auxiliary output or select “None” if the output will be used as a Door Strike.

Time

Select the reader auxiliary output time. This is length of time that the auxiliary relay on the door-controller module will remain energized each time it is triggered.

Activate Output During Timezone

If you want to activate the relay for specific durations, choose the timezone that spans the indicated intervals. Available choices are the currently defined timezones.

Always Activate Output

If this check box is selected, the output will be always activated. This field is not available for CASI panels.

Activate Output

When the main control panel goes into the specified alarm state (In Alarm, Siren, or Area Local Alarm), the output is activated. If “Area Local Siren” is selected, the **Area** drop-down is enabled.

This field is not available for CASI panels.

Note: An output state controlled by a local function takes precedence over an output state configured for the reader or door.

Area

The area that local siren output is associated with. Choose from all areas assigned to the reader’s access panel. This field is not available for CASI readers.

NGP Procedures

To configure an NGP access panel, the following steps must be completed.

1. Configure the NGP network settings. For more information, refer to Configure the NGP Network Settings on page 1568.
2. Add an NGP access panel to the system. For more information, refer to Add an NGP Access Panel on page 1569.
3. Add a door/reader to the NGP access panel. For more information, refer to Add a Door/Reader to an NGP Access Panel on page 1570.
4. Configure an NGP reader for Cardholder Time and Attendance reporting. For more information, refer to Configure an NGP Reader for Cardholder Time and Attendance Reporting on page 1571.
5. Configure an NGP access level to the system. For more information, refer to Configure the NGP Access Level on page 1571.
6. Add an area to the NGP access panel. For more information, refer to Add an Area to an NGP Access Panel on page 1572.
7. Add an area group to the NGP access panel. For more information, refer to Add an Area Group on page 1573.
8. Configure an alarm panel to the NGP access panel. For more information, refer to Configure an Alarm Panel for an NGP Access Panel on page 1573.

Configure the NGP Network Settings

NGP Default Network Settings

Connection	IP	Network Mask	Network Gateway
Primary Ethernet Connection (eth0)	Primary IP address	Primary network mask	Primary network gateway
Secondary Ethernet Connection (eth1)	Secondary IP address	Secondary network mask	Secondary network gateway

Connection	Default IP Address	Default Network Mask	Comment
Primary Ethernet Connection (eth0)	169.254.1.100	255.255.0.0	The 169.254.X.X network is the APIPA

NGP IP Aliasing Settings

Connection	Default IP Address	Default Network Mask	Comment
Primary Ethernet Connection (eth0)	169.254.1.200	255.255.0.0	The 169.254.X.X network is the APIPA
Secondary Ethernet Connection (eth1)	169.254.1.201	255.255.0.0	The 169.254.X.X network is the APIPA

1. Connect a laptop directly into one of the ethernet ports of the NGP access panel. There should be no other network infrastructure between the laptop and the panel.
2. On the laptop, set the APIPA network (169.254.*.*) to be a static network. For more information on how to configure a network see Microsoft Windows help.
3. To view the network setting on the LCD keypad:
   a. Connect a SNAPP LCD keypad to one of the SNAPP busses on the panel.
   b. Log into the keypad using the service PIN. The settings shown are read-only and are only used for troubleshooting.
4. To change the network settings:
   a. Type the following URL into a browser to get to the Network Settings page: `https://169.254.1.100/networkSettings.cgi` where the IP address is replaced with the IP address you are using.

      IMPORTANT: A security exception is required in your browser to allow access to the URL.

   b. A username (service logon) and password (service PIN) are required for the URL. The default information is:
      - Username = 000000
      - Password = 2482
5. On the Network Settings page, update any network information desired and click [Update].

   IMPORTANT: If the URL used was the secondary IP address the browser will not refresh correctly after you click [Update].

6. To configure the IP port and other items, click the Host Communications link at the bottom of the Network Settings page.

Add an NGP Access Panel

1. Display the Access Panels folder by selecting ***Access Panels*** from the ***Access Control*** menu and selecting the NGP tab. Click [Add].

2. In the **Name** field, type a unique, descriptive name for the access panel.
3. If you want to place the panel online immediately, select the **Online** check box. Typically, you wouldn't check this box when configuring the system or defining panels, but instead would wait until you're ready to put the panel into service.
4. Specify communication parameters on the Primary Connection and Secondary sub-tabs.
5. On the Options sub-tab, specify the model of the panel. If the NGP Panel Model selected includes OnBoard Doors then the OnBoard Doors are automatically added. If the CASI Panel Model selected includes Alarm Panels then the Alarm Panels are automatically added.
6. Depending on the panel model, use the other available sub-tabs to configure the card formats, log on/PIN, invalid access, power, equipment, diagnostics, capacity, encryption, intrusion, SIA/CID, IP Central Station, and STU settings for your system.
7. For DirecDoor and M5/M3000 Access Panels only: On the Slots sub-tab, assign device extension boards to the panel's slots as required.

   IMPORTANT: These access panel setup parameters must be completed prior to adding cardholder records to the database, and should not be altered after cardholder records have been added. Changing these settings will result in a full cardholder database download to the panel.

8. Click [OK].

Add a Door/Reader to an NGP Access Panel

Note: When you add or delete doors in a system connected to central station reporting, you must recreate the Central Station Setup report to ensure it matches what is reported by the central station.

1. From the ***Access Control*** menu, select ***Readers and Doors***. The Readers and Doors folder opens.
2. On the General tab, click [Add].
   a. In the **Name** field, enter a unique, descriptive name for the door.
   b. In the **Panel** drop-down, select the NGP access panel the door connects to.
   c. Select the reader type.
   d. If using an offboard type, enter the **Serial number**. If using an onboard type, the doors will automatically get a serial number.
   e. In the **Strike** drop-down, select how the door strike is to behave when a valid card swipe occurs.
   f. Configure any other appropriate options.
   g. Click [OK].
3. Select the Door tab and click [Modify].
   a. Select the door configuration for your system.
4. Select the In Reader tab and click [Modify].
   a. Select t the options for your system.
5. Select the Out Reader tab and click [Modify].
   a. Select the options for your system.
6. Select the Grouping tab and click [Modify].
   a. Select the options for your system.
7. Select the Settings tab and click [Modify].
   a. Select the options for your system.

8. Select the Timing and Alarms tab and click [Modify].
   a. Select the options for your system.
   b. Click [OK].
9. Select the Auxiliary Inputs tab and click [Modify].
   a. Select the options for your system.
   b. (Optional) If you are configuring a door opener, select “Extended request to exit” as the auxiliary input **Mode** to delay the strike. Triggers the automatic door opener if **Extended strike/held times** is enabled for the cardholder. For more information, refer to Badge Form on page 109.
   c. Click [OK].
10. Select the Auxiliary Outputs tab and click [Modify].
    a. Select the options for your system.
    b. (Optional) If you are configuring a door opener, select “Door opener” as auxiliary output **Mode**. Uses the extended strike/held open times specified for the door. For more information, refer to Timing and Alarms Form on page 1564.
    c. Click [OK].

Configure an NGP Reader for Cardholder Time and Attendance Reporting

Note: Only information from NGP out readers is included in the Cardholder Time and Attendance report.

In System Administration, complete the following steps:

1. From the ***Access Control*** menu, select ***Readers and Doors***.
2. On the Settings tab, select the **Is an in/out station (time and attendance)** check box.
3. On the Door tab, select “In and Out Readers” from the **Reader configuration** drop-down.

Configure the NGP Access Level

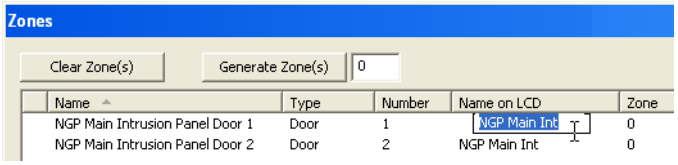
For more information, refer to Chapter 33: Access Levels Folder on page 719.

1. From the ***Access Control*** menu, select ***Access Levels***.
2. On the NGP Intrusion sub-tab, click [Add].
3. In the **Name** field, type a unique, descriptive name for this access level.
4. The **LCD name** field is automatically generated. If you wish, update the name as it will appear on the LCD reader display.
5. In the Areas to assign listing window, select one or more areas that will be assigned to the access level.
6. In the Permission profile to assign listing window, select a permission profile.
7. Click [Assign]. An entry will be inserted into the assignment window for each selected area.
8. To remove one or more areas from this access level:
   a. In the assignment listing window, click on the entry or entries that you want to remove.
   b. Click [Remove]. The entry or entries will be removed from the assignment window.
9. Click [OK].

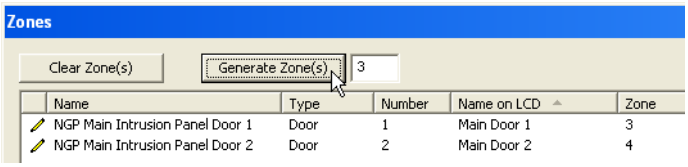
Add an Area to an NGP Access Panel

For more information, refer to Chapter 35: Areas Folder on page 753.

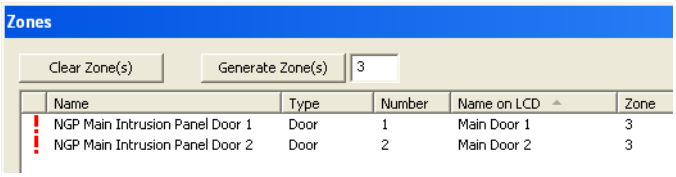
1. Select ***Areas*** from the ***Access Control*** menu. The Areas folder opens.
2. Select the Areas tab.
3. Click [Add].
4. The Add Area window opens.
   a. If using Global Anti-passback, specify if you want to create a global or local area.
   b. Select the NGP panel(s) to be associated with the area.
   c. Click [OK].
5. On the General sub-tab:
   a. In the **Name** field, type a descriptive name for this area.
   b. Configure any **Anti-Passback** options as required by your system.
   c. Configure any **User Counting** options as required by your system.
   d. If configuring a local area, configure any **Activity Detection** options as required by your system.
6. *For NGP Intrusion Panels only.* If configuring a local area, on the Intrusion Detection sub-tab:
   a. Configure any **Delay Times** options as required by your system.
   b. Configure any **Exit Settings** options as required by your system.
   c. Configure any **Other Settings** options as required by your system.
   d. Configure Central Station reporting zones as required by your system.
      - Click [Configure Reporting Zones] for the selected area. The Zones dialog is opened.
      - Double-click on the **Zone or Name of LCD** field of the device you want to update, and then edit the value.



      - If you want to set all zone numbers to zero (0), click [Clear Zone(s)].
      - If you want to generate zone numbers for multiple items, enter a beginning zone number, and then select the devices you want to update. Click [Generate Zone(s)].



   e. Click [OK] to submit the changes.
   f. If a zone number conflict occurs, modify the zone numbers in question, and then click [OK} again. Zone numbers must be unique within an area.



7. If configuring a local area, on the Arming/Disarming sub-tab:
   a. Configure any **Arm/Disarm Scheduling** options as required by your system.
   b. Configure any **Auto Disarm on Valid Token** options as required by your system.
   c. Configure any **Special** options as required by your system.
   d. Configure any **Extended Auto Arm** options as required by your system.
   e. Configure any **Stay Off Stay Scheduling** options as required by your system.
   f. Configure any **Arm/Disarm Common Areas** options as required by your system.
   g. Configure any **Arming/Disarming Priority** options as required by your system.
8. Click [OK].

Add an Area Group

1. Select ***Areas*** from the ***Access Control*** menu. The Areas folder opens.
2. Select the Area Group tab.
3. Click [Add].
4. Enter the **Name** and **Name on LCD** fields.
5. Select the panel associated with the areas you will be assigning to the group.
6. Select the areas to add to the group.
7. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Configure an Alarm Panel for an NGP Access Panel

For more information, refer to Chapter 29: Alarm Panels Folder on page 685.

Notes: When you add or delete alarm panels or alarm inputs in a system connected to central station reporting, you must recreate the Central Station Setup report to ensure it matches what is reported by the central station.

Step 1: Add an Alarm Panel

1. Select ***Alarm Panels*** from the ***Access Control*** menu.
2. On the Alarm Panels tab, select the NGP panel from the listing window and click [Add].
3. Select the panel from the **Panel** drop-down box.
4. In the **Name** field, enter the name of the alarm panel.
5. In the **Serial Number** field, enter the serial number of the alarm panel.
6. In the Capacity section of the form, select the panel **Model** (if available) and enter the number of inputs and outputs that are to be used by the panel.
7. From the **Area** drop-down box, select the area to be associated with the alarm panel.
8. Click [OK].

Step 2: Add an Alarm Input

1. Select the Alarm Inputs tab and click [Add]
2. In the listing window, select the alarm panel that you're adding to the input.
3. In the **Name** field, type a unique and descriptive name for the input.
4. *For NGP Alarm Panels only.* The system will suggest an LCD name to be displayed at the LCD keypad. You can edit this if necessary.
5. Enable or disable the **Online** check box to indicate whether the input should be online.
6. Enable or disable the **Checkpoint** check box if you want the alarm input to be configured as a Checkpoint.
7. Select the **Input Number** that locates this input on the panel.
8. Select a supervision and normally open/closed setting from the **Supervision** drop-down list.

Notes: You can configure up to eight (8) different supervision settings *per* panel.

NGP-1100 alarm panels support up to four (4) different supervision selections *per* panel.

9. Select the **Point Type** that will be used for this input. Non-intrusion panels are pre-configured to "Standard." For more information, refer to Input Point-Type Reference on page 1578.
10. Select the timezone, if any, during which to log events associated with this input.
11. If you want to mask this input during a timezone or always choose the appropriate setting in the Mask Configuration section.
12. Select the **Area**, **Buffer Area**, and **Zone number** that will be associated with this Alarm Panel.
13. Click [OK].

Step 3: Add an Alarm Output

1. Select the Alarm Outputs tab and click [Add]
2. In the listing window, select the alarm panel that you're adding to the output.
3. In the **Name** field, type a unique and descriptive name for the output.
4. Select the output number that locates this input on the panel.
5. Select the duration this output will remain active when directed to pulse.
6. If you want to activate this output during a timezone or always, choose the appropriate setting.
7. If you want to activate this output based on the output condition (In Alarm, Siren, or Local Area Siren state) choose the appropriate setting.
8. Click [OK].

Change Reader Access Modes in Alarm Monitoring

Alarm Monitoring can be used to change the status of the panel and readers of the NGP system. For more information, refer to the Alarm Monitoring User Guide.

To change Reader Access Modes based on the door (both readers):

1. In the system status tree of Alarm Monitoring, Right-click an NGP door/reader.
2. Select Reader Access Modes and choose:
   - **Lock Door** - Select to lock both the in and out reader.
   - **Unlock Door** - Select to unlock both the in and out reader.

- **Reinstate Door** - Select return the door (both the in and out readers) to the Access Modes they were in prior to a recent Lock/Unlock command.

NGP Optional Procedures

The following procedures are optional to configuring an NGP Access panel.

1. Add an NGP Power Supply. For more information, refer to Add an NGP Power Supply on page 1575.
2. Add an NGP User to the system. For more information, refer to Add an NGP User on page 1575.
3. Configure NGP Permission. For more information, refer to Configure NGP Permissions on page 1576.
4. Configure Permission Profiles. For more information, refer to Configure Permission Profiles on page 1576.
5. Configure Local Anti-Passback. For more information, refer to Configure Local Antipassback on page 1577.
6. Add a Local I/O Function List. For more information, refer to Add a Local I/O Function List on page 1577.
7. Add a Global I/O Linkage. For more information, refer to Add a Global I/O Linkage on page 1577.

Add an NGP Power Supply

For more information, refer to Chapter 29: Alarm Panels Folder on page 685.

1. Select ***Power Supplies*** from the ***Access Control*** menu.
2. On the NGP Intelligent Power Supplies tab, click [Add].
3. In the **Name** field, enter the name of the power supply.
4. Select the panel from the **Panel** drop-down box.
5. In the **Serial number** field, enter the serial number of the power supply.
6. Select the area from the **Area** drop-down box.
7. Click [OK].

Add an NGP User

Only an NGP user can perform actions at the keypad. An NGP user should only be configured if someone is required to perform actions at the keypad. For more information, refer to Chapter 3: Cardholders Folder on page 83.

1. Select ***Cardholders*** from the ***Administration*** menu.
2. On the Cardholder tab, click [Add].
3. Enter all of the cardholder data needed.
4. Select the Badge tab and enter the data needed. You must enter a PIN before continuing.
5. Select the Access Levels tab and enter the data needed.
6. Select the NGP User tab.
   a. Click [Assign Next Available] to automatically generate a unique number for the cardholder's **Panel User ID**. The cardholder must have a **PIN** before the **Panel User ID** can be assigned.

b. (Optional) Type a user ID number in the **Panel User ID** field. The system then checks if the number is unique. If not, a message is displayed with a valid range of user ID numbers.

c. Select the panel user language from the **Panel User Language** drop-down.

d. Continue entering the data for all tabs that are needed.

Configure NGP Permissions

The NGP specific permissions allow you to enable or disable users from suspending and resuming arming schedules and allow or disallow configuring permission profiles.

1. To suspend and resume arming schedules:
   a. From the ***Administration*** menu, select ***Users***.
   b. Click the Monitor Permission Groups tab.
   c. Click [Add].
   d. If segmentation is not enabled, skip this step. If segmentation is enabled:

      The Segment Membership window will open. Select the segment that this permission group will be assigned to. Click [OK].
   e. In the **Group Name** field, type a unique, descriptive name for this permission group.
   f. On the Control sub-tabs, the NGP specific permission is: Suspend/resume arming schedules. Enable or disable the permission.
   g. Click [OK].
2. To allow or disallow configuring of permission profiles:
   a. From the ***Administration*** menu, select ***Users***.
   b. Click the System Permission Groups tab.
   c. Click [Add].
   d. If segmentation is not enabled, skip this step. If segmentation is enabled:

      The Segment Membership window will open. Select the segment that this permission group will be assigned to. Click [OK].
   e. In the **Group Name** field, type a unique, descriptive name for this permission group.
   f. On the Intrusion sub-tabs, the NGP specific permission is: Permission profiles. Enable or disable the permission.
   g. Click [OK].

Configure Permission Profiles

IMPORTANT: Before configuring permission profiles you must first add permission profiles permissions. For more information, refer to Configure NGP Permissions on page 1576.

1. Display the Permission Profiles folder by selecting ***Access Levels*** from the ***Access Control*** menu and selecting the Permission Profiles sub-tab.
2. Click [Add]. You can only view permission profiles if an NGP access panel has been added to the system.
3. In the **Name** field, type a unique, descriptive name for the permission profile.
4. Specify the permissions on the General, and Schedule-Based sub-tabs. For more information, refer to Permission Profiles (General Sub-tab) on page 738.
5. Click [OK].

Configure Local Antipassback

This procedure assumes that you have already configured your NGP Access Panel.

1. Configure Areas:
   a. Select ***Areas*** from the ***Access Control*** menu. The Areas folder opens. Select the Areas tab.
   b. In the listing window, select the area that anti-passback will be configured for. Click [Modify].
   c. In the Anti-Passback section of the General sub-tab, select any options as required by your system.
   d. Click [OK].
2. Configure Readers and Doors:
   a. From the ***Access Control*** menu, select ***Readers and Doors***. The Readers and Doors folder opens.
   b. On the In Reader and/or Out Reader tab, choose an anti-passback mode from the **Anti-passback mode** drop-down box.
   c. Click [OK].

Add a Local I/O Function List

For more information, refer to Add a Local I/O Function List on page 796.

Add a Global I/O Linkage

For more information, refer to Add a Global I/O Linkage on page 814.

NGP References

Input Point-Type Reference

Point Type (###)	Class	Monitored for these Area Arming Level(s)	Monitoring Style	By-pass	Chime	Tx Off	Tx Stay	Tx On	SonIrt Off	SonIrt Stay	SonIrt On	Siren Off	Siren Stay	Siren On
01 (Entry Door)	Burg	Stay & On	Entry/Exit Door	–	X	–	X	X	–	X	X	–	X	X
02 (Entry Route)	Burg	ON Only	Entry/Exit Route	X	–	–	–	X	–		X	–	–	X
03 (Perimeter)	Burg	Stay & On	Immediate	X	X	–	X	X	–	X	X	–	X	X
04 (Interior Motion)	Burg	ON only	Immediate	X	–	–	–	X	–		X	–	–	X
05 (Motion–FAP)	Burg	ON only	FAP	X	–	–	–	X	–		X	–	–	X
FAP: (False Alarm Preventor) If a FAP input is not OK longer than 10 seconds, an alarm condition occurs. If a FAP input is triggered and immediately resets, a 20 minute timer begins. If the same device is tripped or a different FAP device trips in the same 20 minutes, an alarm occurs.														
06 (Day Warning)	Burg	24hr	Immediate	X	–	–	–	X	X	X	X	–	–	X
07 (24hr Burglary)	Burg	24hr	Immediate	X	–		X	X	X	X	X	X	X	X
10 (Fire - A)	Fire-A	24hr	Immediate	–	–	X	X	X	X	X	X	X	X	X
11 (Fire - Delayed)	Fire	24hr	15s delay	–	–	X	X	X	X	X	X	X	X	X
12 (Fire - Immed)	Fire	24hr	Immediate	–	–	X	X	X	X	X	X	X	X	X
13 (Hold-up)	Holdup	24hr	Immediate	–	–	X	X	X	–	–	–	–	–	–
14 (Aux Alert)	Emerg	24hr	Immediate	–	–	X	X	X	X	X	X	X	X	X
20 (Supervisory)	Spvsr	24hr	Immediate	X	–		X	X	X	X	X	–	–	–
30 (Local - 24hr)	Burg	24hr	Immediate	X	–	–	–	–	X	X	X	X	X	X
31 (Local-Stay&On)	Burg	Stay & On	Immediate		X	–	–	–	–	X	X	–	X	X
32 (Future Use)	Burg	Future Use	Future Use	X	X	–	–	–	–	–	X	–	–	X

Input Point-Type Reference (Continued)

33 (Local - ON only)	Burg	ON only	Immediate	X	X	–	–	–	–	–	X	–	–	X
46 (Work Late)	Spvsr	ON only	Work Late Function	–	–	–	–	–	–	–	–	–	–	–

Tone Conditions

Condition	Standard Tones	Reverse Tones
Fire	1 Second on and off.	1 second on and off.
Chime	Three 125 ms, short low level beeps	Three 125 ms, short low level beeps
Exit/Entry Delay	Slow turn on/off tones: On Time: 250 ms Off Time: 750 ms	Steady continuous tone
Exit Delay with point open *	Fast turn on/off tones On Time: 250 ms Off Time: 250 ms	Fast turn on/off tones On Time: 250 ms Off Time: 250 ms
Confirm Exit delay	Fast turn on/off tones On Time: 250 ms Off Time: 250 ms	Fast turn on/off tones On Time: 250 ms Off Time: 250 ms
Trouble - Alarm Area Fail to Arm *	Steady continuous tone	Slow turn on/off tones: On Time: 250 ms Off Time:750 ms
Entry delay with was/current in alarm	Very Fast turn on/off tones On Time: 125 ms Off Time: 125 ms	Very Fast turn on/off tones On Time: 125 ms Off Time: 125 ms
Area closing - 15 minutes	Three 125 ms, short tones. Tones faster during last 5 minutes	Three 125 ms, short tones. Tones faster during last 5 minutes

* The tone will NOT be generated if the applicable area's “Fail to Exit Mode” is set to None/0 (zero).

NGP Transmitted Messages (SIA & Contact-ID)

General Message Format

Messages are transmitted to the monitoring station using either the “SIA Level II” or “Contact ID” format.

IMPORTANT: The SIA and CID message formats are NOT to be confused with messages provided by the receiver software. (Receiver software messages typically

include the information discussed here, along with date/time information and proprietary formatting.)

SIA Level 2 Message Format

Format for messages that reference an area: **N riSSSS / XX PPP**

System message format (no area reference): **N XX PPP**

Component	Description
N	This indicates a “new event”.
Ri	This indicates “area” (i.e., the next number is an area reference).
SSSS	This is the area number (ID).
XX	This is the two-character SIA alarm code. For more information, refer to Event Message List (Sorted by SIA Code) on page 1582.
PPP	This is the number (ID) for the input point or user associated with the event, or optional information (depending on the type of event).

Sample Messages	Description
N ri2 / BA 227	Burglar alarm associated with area 2; door 27. For more information, refer to Door Alarms on page 1581.
N ri4 / BA 73	Burglar alarm associated with area 4; input point 73.
N UX2	Digital dialer communications test signal.

Notes: When you create an account message template, enter only the two-digit SIA code. (The “**N**” is processed automatically by the receiver.)

Account number information is sent as another message type, and is automatically understood by the receiver software.

User IDs of 998 or Greater

The SIA message format supports unique user ID numbers up to 997, only. User IDs equal to or greater than 998 will display as “998”. User ID “999” is considered to be the “automatic user” which refers to an event that was triggered by the system.

Contact-ID Message Format

Format for CID messages: **CCCC QEEE GG ZZZ**

Component	Description
CCCC	The account number.
Q	An event qualifier: “1” is a new event (shown as “E” in the Event Message List), and “3” means a restoral (shown as “R” in the list). For more information, refer to Event Message List (Sorted by CID Code) on page 1585.
EEE	This is the three-character CID alarm code.
GG	This is the “area” number (ID).
ZZZ	This is the number (ID) for the input point (zone) or the user associated with the event.

Sample Messages	Description
1234 1110 02 003	Account 1234, Fire Alarm detected in area 02 by input point 003.
1234 1301 01 000	Account 1234, AC trouble (reported as Area 1 by default).
1234 3301 01 000	Account 1234, AC restoral (reported as Area 1 by default).

Note: When you create an account message template, enter only the three-digit CID code. (The leading event qualifier is processed automatically by the receiver.)

User IDs of 998 or Greater

The CID message format supports unique user ID numbers up to 997, only. User IDs equal to or greater than 998 will display as “998”. User ID “999” is considered to be the “automatic user” which refers to an event that was triggered by the system.

Door Alarms

Access-controlled doors report burglar or tamper alarms to the Central Station by area and zone number when an area is armed. When disarmed, **Door Forced Open** and **Door Held Open** alarms will report using the Zone number and the “effective area” of a door along with the appropriate Contact-ID (CID) event message codes. For more information, refer to the Event Message List (Sorted by SIA Code) on page 1582 and the Event Message List (Sorted by CID Code) on page 1585.

The door's effective area for reporting MUST be a local area (entering or leaving). If both areas are local, then the area entering will be used for intrusion reporting.

IMPORTANT: When Global Anti-passback is enabled, at least one area must be local to the panel (to be the used for Intrusion Reporting).

Event Message List (Sorted by SIA Code)

SIA	CID Equivalent	Description	Level
AR	R301	AC Trouble (E003--Restore)	Emergency
AT	E301	AC Trouble (E003)	Emergency
BA	E130	Burglary	Emergency
BR	R130	Burglary --Restore	Emergency
BS	E155	Point-Test Fail	Emergency
BT	E383	Burglary --Tamper	Emergency
CA	R403	Automatic Area On (Scheduled auto-arm on fail to close)	Full
CE	E405	Work late (Closing extended)	Emergency
CF	R402	Turn Area On (Bypass or Forced)	Full
CI	E454	Failed to Close	Emergency
CL	R401	Turn Area On (Normal)	Full
DF	E423	Door Forced Open	Emergency
DG	E422	Second User Authority Granted for Dual Custody	Full
DL	E426	Door Held Open (Door Left Open - Alarm)	Emergency
DR		Door Restored	Emergency
DU	E458	Verify User	Emergency
EE	E134	Fail to Exit Area	Emergency
ER	R143	Module tamper/comms/subst'n (E011--Restore)	Emergency
ET	E143	Module Trouble--tamper/comms/subst'n (E011)	Emergency
FA	E110	Fire or Fire-Class A	Emergency
FR	R110	Fire or Fire-Class A--Restore	Emergency
FT	E380	Fire or Fire-Class A--Tamper	Emergency
HA	E421	Duress Pin	Emergency
JR	E404	Schedule resumed (Stay opened resume)	Emergency
JS	E459	Schedule suspended (Stay opened suspended)	Emergency
JT	E625	Time Changed (E007)	Emergency
LB	E306	Main panel Config Changed (E008)	Emergency
LR	R351	Phone Trouble (E004--Restore)	Emergency
LS	R330	Main panel Program Error (E009--Restore)	Emergency
LT	E351	Phone Trouble (E004)	Emergency

SIA	CID Equivalent	Description	Level
LU	E330	Main panel Program Error (E009)	Emergency
LX	R306	Main panel Config Changed (E008--Restore)	Emergency
MA	E100	Aux. Alert	Emergency
MR	R100	Aux. Alert--Restore	Emergency
MT	E380	Aux. Alert--Tamper	Emergency
NF	R456	Turn Area to Stay (Bypass or Forced)	Full
NK +	R407	Emergency Stay (schedules)	Emergency
NL	R408	Turn Area to Stay (Normal)	Full
NR +	R457	Unauthorized Stay (schedules)	Emergency
OA	E409	Automatic Area Off (SDC5 type points)	Full
OG	R441	Turn Area to Stay from On	Full
OI	R453	Failed to Open	Emergency
OK	E451	Early Open	Emergency
	E450	Emergency Off (Exception O/C)	Emergency
OP	E401	Turn Area Off	Full
PA	E120	Holdup, or;	Emergency
		If PA or E120 is with event code “299” for NGP: Global Lockout Alarm caused by invalid card/PIN use in Area	Emergency
PR	R120	Holdup--Restore, or;	Emergency
		PR or R120 is with event code “299” for NGP: Global Lockout Alarm Restore in Area	Emergency
PT	E380	Holdup--Tamper	Emergency
QA	E140	Vault/Safe	Emergency
QR	R140	Vault/Safe--Restore	Emergency
QT	E380	Vault/Safe--Tamper	Emergency
RB	E380	Module Program Changed (E013)	Emergency
RC	R354	Misc Trouble (E015--Restore)	Emergency
ri	n/a	Area-number reference	Emergency
RN	R380	Module Program Changed (E013--Restore)	Emergency
RO	E354	Misc Trouble (E015)	Emergency
RR	E305	Time Lost (E006)	Emergency
RS	R145	Module Program Error (E014--Restore)	Emergency

SIA	CID Equivalent	Description	Level
RU	E145	Module Program Error (E014)	Emergency
TA	E300	Main panel Tamper (E001)	Emergency
TR	R300	Main panel Tamper (E001--Restore)	Emergency
TS	E607	Walk or Holdup Test Started (no message at end of test)	Emergency
UA	E150	Misc/No Type	Emergency
UR	R150	Misc/No Type--Restore	Emergency
UT	E380	Misc/No Type--Tamper	Emergency
UX0	E354	Digital Dialer Comms Failure (Messages Lost)	Emergency
UX1	E356	Security IP Comms Failure (Messages Lost, Sync Lost, Reset)	Emergency
UX2	E602	Digital Dialer Comms Test	Emergency
XR	R384	Module Battery Low--e.g. wireless xmitr (E012--Restore)	Emergency
XT	E384	Module Battery Low--e.g. wireless transmitter (E012)	Emergency
YC	E333	Security IP Comms Trouble (E016)	Emergency
YK	R333	Security IP Comms Trouble (E016--Restore)	Emergency
YM	E309	No battery (E002)	Emergency
YP	E312	Main panel Fuse Failure (E010)	Emergency
YQ	R320	Main panel Fuse Failure (E010--Restore)	Emergency
YR	R309	No or low battery (E002--Restore)	Emergency
YS	E350	Report Delayed, dialer comms trouble (E005)	Emergency
YT	E302	Low Battery (E002)	Emergency

Event Message List (Sorted by CID Code)

CID	SIA Equivalent	Description	Level
E100	MA	Auxiliary Alert	Emergency
E110	FA	Fire or Fire Class A	Emergency
E120	PA	Holdup, or;	Emergency
		If E120 or PA is with event code “299” for NGP: Global Lockout Alarm caused by invalid card / PIN use in Area	Emergency
E130	BA	Burglary	Emergency
E134	EE	Fail to Exit Area	Emergency
E140	QA	Vault/Safe	Emergency
E143	ET	Module Trouble--tamper/comms/subst'n (E011)	Emergency
E145	RU	Module Program Error (E014)	Emergency
E150	UA	Misc/No Type	Emergency
E155	BS	Point-Test Fail	Emergency
E300	TA	Main panel Tamper (E001)	Emergency
E301	AT	AC Trouble (E003)	Emergency
E302	YT	Low Battery (E002)	Emergency
E305	RR	Time Lost (E006)	Emergency
E306	LB	Main panel Config Changed (E008)	Emergency
E309	YM	No battery (E002)	Emergency
E312	YP	Main panel Fuse Failure (E010)	Emergency
E330	LU	Main panel Program Error (E009)	Emergency
E333	YC	Security IP Comms Trouble (E016)	Emergency
E350	YS	Report Delayed, dialer comms trouble (E005)	Emergency
E351	LT	Phone Trouble (E004)	Emergency
E354	UX0	Digital Dialer Comms Failure (Messages Lost), or;	Emergency
	RO	Misc Trouble (E015)	Emergency
E356	UX1	Security IP Comms Failure (Messages Lost, Sync Lost, Reset)	Emergency
E380	FT	Fire Class A--Tamper, or;	Emergency
E380	FT	Fire--Tamper, or;	Emergency
E380	PT	Holdup--Tamper, or;	Emergency

CID	SIA Equivalent	Description	Level
E380	MT	Aux. Alert--Tamper, or;	Emergency
	QT	Vault/Safe-Tamper, or;	Emergency
	UT	Misc/No Type--Tamper, or;	Emergency
	RB	Module Program Changed (E013), or;	Emergency
E383	BT	Burglary --Tamper	Emergency
E384	XT	Module Battery Low--e.g. wireless transmitter (E012)	Emergency
E401	OP	Turn Area Off	Full
E404	JR	Schedule resumed (Stay opened resume)	Emergency
E405	CE	Work late (Closing extended)	Emergency
E409	OA	Automatic Area Off (SDC5 type points)	Full
E421	HA	Duress Pin	Emergency
E423	DF	Door Forced Open	Emergency
E422	DG	Second User Authority Granted for Dual Custody	Full
E426	DL	Door Held Open (Door Left Open - Alarm)	Emergency
	DR	Door Restored	Emergency
E450		Emergency Off (schedules)	Emergency
E451	OK	Early Open	Emergency
E453	OI	Failed to Open	Emergency
E454	CI	Failed to Close	Emergency
E458	DU	Verify User	Emergency
E459	JS	Schedule suspended (Stay opened suspended)	Emergency
E602	UX2	Digital Dialer Comms Test	Emergency
E607	TS	Walk or Holdup Test Started (no msg at end of test)	Emergency
E625	JT	Time Changed (E007)	Emergency
R100	MR	Auxiliary Alert--Restore	Emergency
R110	FR	Fire or Fire-Class A--Restore	Emergency
R120	PR	Holdup--Restore	Emergency
		If R120 or PR is with event code “299” for NGP: Global Lockout Alarm Restore (caused by invalid card/PIN use in Area)	Emergency
R130	BR	Burglary --Restore	Emergency
R140	QR	Vault/Safe--Restore	Emergency

CID	SIA Equivalent	Description	Level
R143	ER	Module tamper/comms/subst'n (E011--Restore)	Emergency
R145	RS	Module Program Error (E014--Restore)	Emergency
R150	UR	Misc/No Type--Restore	Emergency
R300	TR	Main panel Tamper (E001--Restore)	Emergency
R301	AR	AC Trouble (E003--Restore)	Emergency
R306	LX	Main panel Config Changed (E008--Restore)	Emergency
R309	YR	No/Low battery (E002--Restore)	Emergency
R320	YQ	Main panel Fuse Failure (E010--Restore)	Emergency
R330	LS	Main panel Program Error (E009--Restore)	Emergency
R333	YK	Security IP Comms Trouble (E016--Restore)	Emergency
R351	LR	Phone Trouble (E004--Restore)	Emergency
R354	RC	Misc Trouble (E015--Restore)	Emergency
R380	RN	Module Program Changed (E013--Restore)	Emergency
R384	XR	Module Battery Low - e.g. wireless transmitter (E012--Restore)	Emergency
R401	CL	Turn Area On (Normal)	Full
R402	CF	Turn Area On (Bypass or Forced)	Full
R403	CA	Automatic Area On (Scheduled auto-arm on fail to close)	Full
R407	NK +	Emergency Stay (schedules)	Emergency
R408	NL	Turn Area to Stay (Normal)	Full
R441	OG	Turn Area to Stay from On	Full
R456	NF	Turn Area to Stay (Bypass or Forced)	Full
R457	NR +	Unauthorized Stay (schedules)	Emergency

APPENDIX M

PX Panel Integration

All PX panel variants and versions from v4.30 are supported in OnGuard. The panel connection to OnGuard can be Ethernet or Serial. The OnGuard license must support Intrusion Detection devices.

To add a PX panel to OnGuard:

Step 1: Configure Panel Host Communication on page 1589

Step 2: Configure Devices in OnGuard on page 1590

Step 3: Configure PX Panel in OnGuard on page 1591

Step 4: Configure Global Linkage in OnGuard on page 1592

Step 5: Download Database to the Panel from OnGuard on page 1592

Step 1: Configure Panel Host Communication

To configure the Guardall panel connection to OnGuard you must have access to a system keypad. Each of the following edit modes must be configured for the OnGuard integration to perform properly:

1. Using the PX Keypad:
   a. Connect the keypad to XIB bus of the panel.
   b. Power on the panel.
   c. On the keypad, input 0202. If there is a logged event then click [x] to go through and press the checkmark button to reset.
   d. On the keypad, input 05 to go to engineer mode.
   e. When the engineer mode is displayed, input the engineering PIN code.
   f. If there is a logged event then click [x] to go through and press the checkmark button to reset.
   g. On the keypad, input 99 to go to the full menu.
2. Configure Connections

   For Serial Connections:

Note: If you are using panel types PX500HS or PX250HS then be aware that there is no COM port so a W76068 serial module is needed for serial connections. To configure the serial module for the PX500HS or PX250HS then, use the keypad and select Option 13=SM, set SM1 to be Serial, and set the baud rate 9600.

a. In the engineer mode, select option 13.
b. Configure SM0 to use a serial connection, set the baud rate 9600, and configure SM1and SM2 to OFF.
c. Select Option 12 GSR
d. Select GSR1 and set Enable to be Auto, input the S/N (which must be the same as the Dongle number discussed in Step 2: Configure Devices in OnGuard on page 1590), and set the GSR ID to be any 4-digit number.
e. Select Option 11 Tel Number. Leave it to be OFF
f. Connect the panel to the OnGuard system via a COM cable.

For LAN Connections:

g. Link the data comm module to the XIB bus of panel. Connect this module to the same subnet with the system running OnGuard.
h. In the engineer Menu, select option 13.
i. Configure SM1 as ethernet and SM0 and SM2 to be OFF (PX500HS and PX250HS do not have the SM0 option.)
j. Select Option 12 GSR.
k. Select GSR1 if needed. Select GSR1 and set Enable to be Auto, input the S/N (which must be the same as the Doggle number discussed in Step 2: Configure Devices in OnGuard on page 1590),set the GSR ID to be any 4-digit number, and set the IP Address to be the IP address of the system running OnGuard.
l. Select Option 11 Tel Number. Leave it to be OFF
m. Select Option 20 System Option.
n. Go to 10, 11, 12 to set the IP address, Gateway IP, Subnet Mask of the data comm module.

Step 2: Configure Devices in OnGuard

1. Add an Intrusion Panel. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***. The Intrusion Detection Configuration folder opens.
2. On the Intrusion Panels tab, click [Add].
3. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this intrusion panel will be assigned to.
   b. Click [OK].
4. In the **Name** field, type an intrusion panel name.
5. On the Location sub-tab:
   a. Select the **Workstation** to which the intrusion panel is connected to. The Communication Server must be running on the specified workstation.
   b. Select the world time zone from the **World time zone** drop-down list.
   c. Select whether **Daylight savings** is used or not.

Note: The workstation name is obtained from Microsoft Windows by right-clicking the My Computer desktop icon and selecting **Properties**. The workstation name is located on the Computer Name tab.

6. Select the “Guardall EMEA” from the **Intrusion detection panel type**.
7. On the Connection sub-tab.

   If using a LAN connection:

   a. Select the **LAN** radio button.
   b. Enter the IP address and port number. The port number is typically set to 6000.

   If using a Direct connection:

   c. Select the **Direct** radio button.
   d. Set the baud rate to 9600. A crossed RS232 cable should be used to connect the panel to the computer.
8. On the Options sub-tab.

   IMPORTANT: If using the Guardall panels after upgrading from the accessory add-on you may have to re-enter the dongle number and panel model in the **Dongle Number** field and **Panel model** drop-down.

   a. Enter the dongle number in the **Dongle number** field. The dongle number can be any number up to 10 digits. The dongle number must also be programmed in each PX panel that will be connected to OnGuard.
   b. Select the panel model from the **Panel model** drop-down.
9. Click [OK].
10. The zones, areas, doors and offboard relay tabs will be automatically updated when you edit the PX Configuration using the PX Config Tab. Items mapped from the PX panel to OnGuard:
    - Circuit = Zone
    - Output = Offboard relays
    - Group/Area = Area
11. Start the communication Server on the workstation.
12. The panel should appear as online in Alarm Monitoring.

Step 3: Configure PX Panel in OnGuard

Note: The Guardall PX Config tab can only be used after the panel is online. The functionality of the Guardall PX Config tab is the same as that in keypad. The following options are essential for panel to communicating with OnGuard. When modify them please make sure that their values are consistent with that in keypad: Tel Number, GSR , SM, Panel IP, Gateway IP, Subnet Mask.

1. From the ***Additional Hardware*** menu, select ***Intrusion Detection Devices***.
2. Click the Guardall PX Config tab.
3. In the listing window, select the Guardall panel that you want to configure.
4. Select an option from the drop-down box and configure any appropriate options.
   a. Click [Modify].
   b. In order to save panel configuration changes automatically to the databases the "System Size" option in the drop-down list needs to be selected at least once for each panel. Selecting

"System Size" will write the initial values of Zones, Offboard Relays, Doors and Areas. The first time a configuration item is chosen the application will write the default data to the database. Due to the large size of some of the configuration items this process can take a few minutes to complete.

Notes: For alarm reporting to OnGuard the essential menus are:

Alarm Rpt - setup the types of events for each area that will be reported.

Circuits - must be programmed with an appropriate response.

Other useful menus that will be used are:

Set Group - this is the equivalent of an area.

Output Functions - this menu allows mapping of the OnGuard Offboard Relays and the panel output (the physical location on output must be mapped using the appropriate menu.

5. Click [OK].

Step 4: Configure Global Linkage in OnGuard

The Global Linkage feature allows input events to be mapped to output actions. For example, a global linkage could be setup so that when an alarm is received an output on a relay is activated.

For more information, refer to Add a Global I/O Linkage on page 814.

Step 5: Download Database to the Panel from OnGuard

Note: The Guardall PX Config tab can only be used after the panel is online. The functionality of the Guardall PX Config tab is the same as that in the keypad. The following options are essential for the panel to communicate with OnGuard. Before performing a database download please make sure that their values are consistent with that in the keypad: Tel Number, GSR , SM, Panel IP, Gateway IP, Subnet Mask.

To start downloading database to panel, either one of following three ways can be used:

- In the Intrusion Panel tab, right click the panel to be downloaded and select "Download".
- In System Administration, navigate to the Administration menu and select "Download Entire System". Database will be downloaded to all the panels connected with this OnGuard.
- In Alarm Monitoring, right click the panel to be downloaded to and select "Download Database".

Troubleshooting

Trace

To switch on tracing: add the following lines to the **ACS.INI** file

```
[PX]
```

```
PXDebug=1
DebugFileName=c:\temp\Trace.txt
```

Errors

Errors	Cause
Error 0x8007007E, given in the communication Server:	The file in the Device Translator registry key doesn't exist [Check the file is there and the path is spelt correctly]. Make sure the path is C:\Program Files\OnGuard\GuardallTranslator.dll"
Error 0x80040154, given in the communication Server:	The Device Translator registry key doesn't exist [Check the ID number is correct in the registry], the Class is not registered.
Error 0x800736B1, given in the communication Server:	The "Microsoft Visual C++ 2008 Redistributable Package" has to be installed.

Index

Symbols

"D" protocol 1042
example 1045
message format 1042
standard command set 1043

Numerics

75-bit PIV card format 259

A

Access control card formats for ILS locks 1499
Access Control menu 64
Access Groups form
procedures 735
Access Level Additional Segments form
procedures 728
Access levels
assign extend options 726
assign to a badge 118
assign to cardholder group 121
Access levels extended options
non-segmented system 408
segmented system 471
Access Levels folder
Access Groups form 734
Access Level Additional Segments form 727
Access Levels form 719
Elevator Control form 730
Extended Options form 729
Precision Access form 735
Access levels form 197
Access Levels form (Access Levels folder) 719
Access Levels form (Cardholders folder) . 117
procedures 118
Access Panels folder 541
Accounts 51
Acknowledgment Actions form 875
procedures 877
ACS.INI file
encoding section 1443
Action Group Library form 526
overview 525
Action Group Properties window 1196
Action groups overview 525
Action History/Guard Tour Event Purging Properties window 1198
Actions 1193
Activate master keys
non-segmented system 416
segmented system 479
Activation dates assign 120
Active badge synchronization settings 446
Active visit synchronization settings 446
Active visits 152
Activity detection 759
Add
action group 526, 1197
action history/guard tour event purging action 1199
archive/purge database action 1200
area (Areas folder) 768
arm/disarm area action 1202
asset 182
asset groups and classes 187
asset type/subtype 183
audio clip record 866
automatic e-mail message 874
automatic guard tour action 1204
automatic page message 874

badge template 199
badge type 311
bulk badge templates 202
camera 963
cardholder permission group 366, 373
cardholder record 103
CCTV instruction record 869
CMS badge type 1459
CMS connection 1457
CMS smart card format 1459
custom alarm 856
DataConduIT Device 1173
DataConduIT message queue 495
DataConduIT Source 1170
DataConduIT Sub-Device 1175
DataExchange script action 1208
deactivate badge action 1209
device output action 1210
device output group action 1212
dialup modem record 704
directory 341
elevator mode action 1217
elevator terminal allowed floors action 1213
elevator terminal mode action 1214
entry to a list 483
EOL resistor table 823
event routing group 889
event settings 1006
execute function list action 1216
field/page viewing permission group 375
fire device 1057
fire input/output 1059
fire panel 1054
global APB system/segment reset action 1218
global I/O linkage 814, 1577
grant/deny popup action 1220
guard tour 896
HID access panel 625
holiday 707
ILS offline lock 1500
ILS offline operator 1498
ILS offline panel 1498
ILS wireless locks 1520
Integra lock 1482
Integra operator 1478, 1481
intercom call action 1222
intrusion panel 1129
IP camera(s) firmware download action 1263
ISC database download action 1224
ISC firmware download action 1225
LNL-1000 access panel 606
LNL-2000 access panel 594
LNL-2210 access panel 579
LNL-2220 access panel 568
LNL-3300 access panel 555
LNL-500 access panel 618
local I/O function list 796
Magnetic card format 251
mask/unmask alarm input action 1229
mask/unmask alarm input for group action 1231
mask/unmask alarm mask group action 1232
mask/unmask door action 1234
mask/unmask door forced open action 1235
mask/unmask door forced open for reader group action 1237
mask/unmask door held open action 1239
mask/unmask door held open for reader group action 1240
matrix switcher 1038
matrix switcher type 1040
monitor permission group 370
monitor zone 884
monitoring assignment 887
muster mode initiation action 1228
OPC connection 1180
open/close APB area action 1242
paging device 533
panel user group 1146
personal safety panel 1079
pulse open door action 1243
pulse open door group action 1244
reader mode action 1246
reader mode group action 1248
receiver 1103
receiver account 1108
receiver account group 1111
recipient 537
report 210
reset use limit action 1250
run PTZ tour action 1251
schedule report action 1253
set forwarding station action 1259
sign out visitor action 1260
silence area action 1262
SkyPoint Base Server 987
smart card format
- Credential Agent 261
- GSC (iCLASS) 263
- HandKey (iCLASS) 265
- HandKey (MIFARE) 267
- HID (iCLASS) Access Control 269
- IrisAccess (iCLASS) 282, 284
- Lenel (iCLASS) 276
- Smart Card CSN 279
- SmartID (MIFARE) 274
- V-Smart 289

SNMP Agent 1162
SNMP Manager 1159
special instructions 902

system permission group 363
text library entry 498
text record 864
timezone 710
tour group 904
transmitter 1084
transmitter input 1088
user 350
video recorder 935
virtual matrix switcher 1038
visit record 154
visitor record 106
Wiegand card format 257
workstation entry 381
zone 1114
Add an ILS wireless access panel 1519
Add e-mail message window 872
Add Operator dialog 1494
Add pager message window 872
Add Recipient window 165
Adding (Modifying) Recipient Address form 535
Adding (Modifying) Recipient form 535
Additional Hardware menu 67
Administration menu 62
Advanced segmentation 1413
Alarm - Video Configuration form 980
procedures 984
Alarm Acknowledgment Reports form 229
Alarm Configuration folder 849
Alarm Configuration form 858
Alarm Definitions form
modify mode for normal events 851
modify mode for parameter-based events 851
procedures 855
view mode 850
Alarm descriptions 1265
Alarm inputs
Alarm Inputs form 689
procedures 693
Alarm Monitoring
CMS events displayed in 1462
Alarm outputs
procedures 696
Alarm Panel Reports form 215
procedures 217
Alarm Panels folder 685
Alarm Outputs form 694
Alarm Panels form 685
Input/Output Local Linkage form 697
Alarm panels for elevator readers 676
Alarm Panels form
procedures 688
Alarm priority-define range 862
Alarm shunt and pre-alarm compatibility 648, 650
Alarm/event descriptions 855
Analog video capture 1368
Anti-Passback Areas form 756
procedures 767
Anti-Passback form 666
procedures 668
Anti-Passback Reports form 218
procedures 221
Application menu 60
Application_Configuration_Wizards 78
Apply
motion mask to a camera 967
Archive database records 507
Archive Server form 988
procedures 990
Archive/Purge Database Properties window 1199
Archives folder 501
Archiving form 503
Areas folder 753
Areas form (Intrusion Detection Configuration folder) 1140
procedures 1141
Areas form (Receivers folder) 1115
procedures 1117
Arm 1201
Arm/Disarm Area Properties window 1200
Arm/Disarm Command
overview 1469
ASCII
Select Decimal ASCII Code dialog 298
ASCII character chart 1429
ASCII protocol example 1045
Asset classes
add 186
Asset Classes form 184
procedures 186
Asset groups
add 186
Asset menu 71
Assets
assign to cardholder 130
Assets form
Cardholders folder 130
procedures 130
Assets form (Assets folder) 178
procedures 181
Assign
access level(s) to a user 350
access levels example 1419
cardholder to an asset 191
checkpoint actions 898
classes to an asset 186
monitor zone to a user 350
monitoring stations to a tour 901
transmitter input to an asset 1088
transmitter to a cardholder 1085
transmitter to an Asset 1086

Assign Intrusion Authority to the Cardholder 119
Assignments form 189
procedures 190
Associated Inside Areas form 771
procedures 772
Associated Safe Locations form
field table 770
procedures 771
Audio form 865
procedures 866
Audio Level event 1019
Authorization warning configure 396
Automatic cropping 1356
image requirements for 1357
Automatic encryption
configure (non-segmented system) .. 414
configure (segmented system) 477
Automatic gain control 1001
Automatic Guard Tour Properties window 1202
Automatic image rotation 1357
Automatic Lookup form 441
Aux Inputs form 656
procedures 659
Aux Outputs form 659
procedures 661
Auxiliary Server form 986
procedures 987

B

Badge form 109
procedures 114
Badge ID
generate badge ID options 326
Badge ID allocation
all badge types 443
configure for specific badge type 325
Badge ID Allocation form
Badge Types folder 320
Cardholder Options folder 429
Badge status in CMS 1467
Badge template form 195
procedures 199
Badge templates 195
Badge templates for ILS 1491
Badge type
assign encoding format 318
configure ID allocation 443
specify required fields 320
Badge type classes 312
Badge Type form 307
procedures 311
Badge type segmentation 1416
Badge Types folder 307
Badge Type form 307
Deactivation Settings form 329
Encoding form 316
Logical Access form 328
Printing form 314
Required Fields form 319
Segment Membership form 313
Badges
add or replace record 114
assign access levels 118
assign precision access group 126
encode 116
synchronize active badges with visits 445
synchronize summary table 446
Barcodes
CAC 91
configuring to read CAC barcodes 91
scanning with a wedge scanner 91
Binary protocol example 1045
Bind
CMS card 1464
PIV card with CMS 1465
Biometrics
procedures (non-segmented system) 403
procedures (segmented system) 467
search records 127
Biometrics form
Cardholders folder 126
procedures 127
Bioscrypt
security level acceptance/rejection rates 468
Bits per pixel table 1379
Blind Camera event
automatic gain control 1001
Blind camera event
configuration/search dialog 1000
overview 1000
Blocking cards for Integra locks 1488
Brightness Change event
configuration/search dialog 1002
overview 1002
Build a custom expression - process outline 299
Bulk badge template configuration form .. 201
Bulk unassign cardholders 202
Bus devices 1074
Bypass preview scan step 1372

C

CAC barcodes 91
Calculate maximum cardholders for ILS lock 1504
Camera form
Audio sub-tab 956
Capacity sub-tab 959
Communication sub-tab 940
Connection sub-tab 942
Event Mode sub-tab 953
Event Recording sub-tab 953
In-camera storage sub-tab 957
Normal Mode sub-tab 951

procedures 962
add camera with LNVR recorder 962
add LDVR, Generic Video or Loronix cameras 963
Quality sub-tab 946
Record settings sub-tab 944
Video sensor sub-tab 949
Video sub-tab 947
Camera Inputs form 969
procedures 970
Camera Outputs form 972
procedures 973
Capture
digital image 1374
fingerprint (Bioscrypt) templates ... 1385
hand print templates 1382
IrisAccess templates 1395, 1398
Capture individual finger 1391
Capture multiple fingers 1391
Capture tips
Iris (IrisAccess 3000) 1395
Capture Video on Demand 966
Capture Video on Event 965
Card format segmentation 1416
Card formats
CMS 260, 1459
Credential Agent 261
GSC (iCLASS) 262
hid access control (iclass) 267
hid access control (mifare) 270
IrisAccess (iCLASS) 279
Magnetic 248
prioritize for reader 1500
SmartID (MIFARE) 272
V-Smart (iCLASS) 286
V-Smart (MIFARE) 286
Wiegand 252
Card formats for ILS locks 1499
Cardholder
capture photo from live video 1363
capture signature 1361
Cardholder form 98
procedures 103
Cardholder menu 69
Cardholder Options 1458
Cardholder options configure 442
Cardholder Options folder 423
Automatic Lookup form 441
Badge ID Allocation form
ID Allocations sub-tab 427
ID Ranges sub-tab 430
Cardholder Search Results Lists form 434
General Cardholder Options form 423
Logical Access form 434
Person E-mail Fields form 439
Visit Notification Fields form 438
Visit Search Results Lists form 437
Visitor Search Results Lists form 436
Visits form 431
Cardholder Permission Groups form
overview 364
permissions tree 365
procedures 366
Cardholder Search Results Lists form 434
Cardholder segmentation 1417
Cardholders
assign access levels to cardholder group 121
destroy all data 104
modify segment assignments 108
retrieve recent search results 89
run reports 135
search for cardholders 88
Cardholders folder 83
Access Levels form 117
ILS Authorization form 137
procedures 87
CCTV Instructions form 867
Change
user password 50
Change Network Video Password Properties window 1204
Checkpoints assign checkpoint actions 898
Choosing 1420
Chromakey sub-tab 1345
procedures 1346
Cipher mode 638
CMS
add badge type 1459
add CMS smart card format 1459
add connection 1457
Card Format form 260
configure encoder 1461
configure workstation 1461
events displayed in Alarm Monitoring 1462
integrating with 1453
licenses 1456
Logical Access form 328
policy 328
using with OnGuard 1455
verify connectivity to 1458
Color form 861
Color information table 1379
Color of disabled text 57
Command Programming form 669
procedures 671
Communication paths used by receivers 1094
Compare permissions 360
Comparison operators 87, 151
Compress a captured image 1359
Confgure panels or readers from the Application wizards 78
Configure 963

acknowledgment actions 877
ActivIdentity Cardholder Options .. 1458
alarm 860
archive parameters 506
area 1141
associated inside area 772
associated safe location 771
authorization warning 396
Badge layout to encode JIS II magnetic stripe 1448
camera 963
cardholder search results lists 447
commands to execute by icon type .. 908
destination assurance 827
FlashPoint/MCI video capture settings 1368
gates 488
ILS cardholder authorization assignments 1491
ILS custom encoding 1487
ILS iCLASS printing and encoding 1513
Integra blocking cards 1488
Integra locking system 1480
Integra system options 1485
Integra timezones 1489
multimedia capture module for file import 1375
muster reporting 774
offboard relays 1138
personal safety device 1090
perspective correction 1030
SMTP server settings 531
special purpose card 1511
special purpose cards 1511
system options for ILS wireless locks 1522
system's force protection setting 486
use or lose badge type settings 331
user permissions 356
video channel parameters 1032
WDM video settings 1363
wedge scanner 94
Configure an ILS offline locking system 1497
Configure an ILS wireless locking system 1518
Configure ILS priority one events 1524
Contact-ID (CID) message format 1581
Control characters in CCTV command strings 869
Controller encryption
Master Key Entry window (non-segmented system) 413
Master Key Entry window (segmented system) 476
procedures (non-segmented system) 414
procedures (segmented system) 477
Controller Encryption form
automatic key management encryption 411
manual key management encryption 411
plain connection 411
Controls form 651
procedures 655
Conventions used in this documentation 49
Create
input-to-output link 698
messages and link them to checkpoint events 899
Creating New (Modifying) Recipient window 535
Creating New Recipient Address window 535
Credential Agent card format 261
Crop window
move 1358
resize 1358
Cross Match ID 500 functionality 1387
Custom Authorization Text window 395
Custom command grammar
direct PTZ systems 1042
matrix-based systems 1040
Custom encoding example 300
Custom event code templates-procedures 1121

D

Data entry forms 79
Data integrity 507
Database Field Properties window
blank 294
date/time 295
text/numeric 296
DataConduIT Devices form
field table 1173
procedures 1173
DataConduIT Message Queues form
Advanced sub-tab 494
General sub-tab 492
procedures 495
Settings sub-tab 493
DataConduIT Sources
licenses required 1168
user permissions required 1169
DataConduIT Sources form 1169
field table 1170
procedures 1170
DataConduIT Sub-Devices form
field table 1175
procedures 1175
DataExchange Script Properties window 1207
Date/Time Reports form 222
procedures 225
Deactivate Badge Properties window 1208
Deactivate date minimum/maximum 620
Deactivation dates assign 120
Deactivation Settings form 329
procedures 331
Default e-mail recipients
configure (non-segmented system) .. 407

configure (segmented system) 471
Default Icon Commands form 907
procedures 908
Default receiver configuration 1095
Default settings 1344
Default text color 57
Delete
action group 528
alarm definition record 858
alarm priority range 863
archive file from the system 511
area (Areas folder) 768
asset 182
audio clip record 867
automatic message 875
badge in OnGuard 1467
badge record 117
badge type 313
card format 304
cardholder permission group 366, 373
cardholder record 104
CCTV instruction record 869
DataConduIT Device 1173
DataConduIT message queue 496
DataConduIT Source 1171
DataConduIT Sub-Device 1175
directory 342
effect profile 1353
entry from a list 483
event routing group 890
field/page viewing permission group 376
fire device 1057
fire input/output 1059
fire panel 1055
global I/O linkage 815
HID access panel 625
holiday 708
intrusion panel 1131
LNL-1000 access panel 607
LNL-2000 access panel 595
LNL-2210 access panel 580
LNL-2220 access panel 569
LNL-3300 access panel 556
LNL-500 access panel 619
local I/O function list 797
matrix switcher 1038
matrix switcher type 1040
monitor permission group 370
monitor zone 885
monitoring assignment 887
OPC connection 1181
paging device 534
panel user group 1147
personal safety panel 1080
receiver 1104
receiver account 1109
receiver account group 1112
recipient 538
report 210
restored records from the database .. 513
scheduled action using the scheduler right-click menu 523
selected group of cardholder records 104
SNMP Agent 1163
SNMP Manager 1160
system permission group 363
text library entry 499
text record 865
timezone 711
transmitter 1085
transmitter input 1088
transmitter's assignment 1086
user 353
user/cardholder in OnGuard 1467
visit record 158
visitor record 107
workstation entry 382
zone 1115
Dependenices 360
Destination assurance
configure 827
segmented systems 825
Destination Assurance folder 825
Destination Assurance form 826
procedures 827
Destroy all cardholder data 104
Details form 163
Device - Camera Links form 977
procedures 978
Device --> Function Links form 797
procedures 798
Device Configuration form 1088
procedures 1090
Device Groups form
procedures 788
view mode 786
Device Output Group Properties window 1211
Device Output Properties window 1209
Dialup Configuration folder 701
Digital camera procedures 1374
Digital Camera Settings sub-tab 1373
Digital image capture 1374
Digital Video folder 911
Alarm - Video Configuration form .. 980
Archive Server form 988
Auxiliary Server form 986
Camera form 939
Camera Outputs form 972
Device - Camera Links form 977
PTZ Tour Server form 994
Security form 992
Video Processing form 994, 998
Video Recorder form 924
Directories 335
overview 335

Directories form
Advanced sub-tab ... 340
Authentication sub-tab ... 339
General sub-tab ... 335
procedures ... 341
Directory account link ... 131
Directory Accounts form ... 131
procedures ... 131
Disable a user account ... 353
Disable strong password enforcement ... 50
Disabled text color-change ... 57
Display
scheduler right-click menu ... 521
system tree ... 73
system tree menu ... 76
Display/hide text labels on toolbar buttons 72
Dock/undock the system tree ... 76
Door alarms ... 1581
Doors form ... 1138
procedures ... 1139
Double video on alarm ... 983
Download
ILS system options ... 1486
ILS wireless firmware ... 1524
Integra locks ... 1483
maximum cardholders supported by ILS locks ... 1502
Download command ... 1503
Download ILS Locks ... 1505
Download panels and locks ... 1502
Download to Portable Device command 1503
Dual readers
addresses ... 637
reader number ... 637
Duress
fingerprint (Bioscrypt) templates ... 1386

E

Edit menu ... 61
Effect profile
create ... 1352
delete ... 1353
modify ... 1352
Effects Gallery sub-tab ... 1347
procedures ... 1351
Elevator Control form
procedures ... 732
Elevator dispatching additional controls
configuration instructions ... 837
Elevator Hardware form ... 672
procedures ... 674
Elevator Terminal Allowed Floors Properties window ... 1212
Elevator Terminal Mode Properties window ... 1214
Elevators
control limits ... 674
floor tracking ... 676
standard control mode (no floor tracking) ... 675
E-mail Fields form ... 439
E-mail form ... 164
E-mail recipients
configure (non-segmented system) .. 407
configure (segmented system) ... 471
Enable
encryption for LNL-1000 ... 607
encryption for LNL-2000 ... 595
encryption for LNL-2210 ... 580
encryption for LNL-2220 ... 569
encryption for LNL-3300 ... 556, 569
encryption for LNL-500 ... 619
Enable strong password enforcement ... 50
Encode
badges ... 116
CMS card ... 1464
PIV card with CMS ... 1465
smart cards with Bioscrypt templates ... 1387
smart cards with IrisAccess templates and access control information 1396, 1399
Encoders
configure ... 388
overview ... 382
Encoders form
Communications sub-tab ... 385
Encoding sub-tab ... 388
General sub-tab ... 384
Location sub-tab ... 385
procedures ... 388
Encoding form (Badge Types folder) ... 316
procedures ... 318
Encryption
Master Key Entry window (non-segmented system) ... 413
Master Key Entry window (segmented system) ... 476
procedures (non-segmented system) 414
procedures (segmented system) ... 477
Enter notes
HID access panel ... 625
LNL-1000 access panel ... 608
LNL-2000 access panel ... 596
LNL-2210 access panel ... 581
LNL-2220 access panel ... 570
LNL-3300 access panel ... 557
LNL-500 access panel ... 620
EOL Resistor Tables form ... 820
advanced custom type tables ... 821
basic custom type tables ... 821
procedures ... 823
EOL Tables folder ... 819
Ericsson MD110 intercom communication ... 1061
Error messages ... 51

Escort mode
assign to access level 726
enable (non-segmented system) 409
enable (segmented system) 472
Event code mappings overview 1096
Event Code Templates form 1118
procedures 1121
Event Configuration/Search
dialog 1023
open dialog 1028
procedures 1028
Event descriptions 1265
Event logging and reporting overview 1096
Event properties 1029
Event recording
increase frame rates 966
Event Reports form 226
procedures 229
Event Routing form
procedures 889
view mode 888
Event settings - add 1006
Events overview 1096
Execute Function List Properties window 1215
Export
images 1344
Export master keys
non-segmented system 416
segmented system 478
Extended Held Command
segmented system 469
Extended Options
assign 726
Extended options for access levels
enable (non-segmented system) 409
enable (segmented system) 472

F

Facility code-determine 259
Failover
overview 920
Failure to Acknowledge Form 877
Field/Page Permission Groups form 374
procedures 375
File I/O Settings sub-tab 1374
Filter report view 211
Find cardholder/visitor associated with a visit 154
Fingerprint
enrollment 1383
images 1383
overview 1383
templates 1383
verification 1383
Fingerprint (Bioscrypt)
capture templates 1385
functionality 1384
license 1384
permissions 1384
verify templates 1386
Fingerprint (Bioscrypt) form 1383
Finished visits 152
Fire Devices form 1056
procedures 1057
Fire Inputs/Outputs form 1058
procedures 1059
Fire Panels folder 1049
Fire Panels form
Connection sub-tab 1051
Encryption sub-tab 1053
Location sub-tab 1050
Notes sub-tab 1053
Options sub-tab 1052
procedures 1054
First card unlock 1245, 1247
authority required 647
LNL-1000 603
LNL-2000 591
LNL-2220 565
LNL-3300 552
LNL-500 615
Readers folder 638
timezone/reader mode 713
Fixed ID range
procedures (all badge types) 444
procedures (per badge type) 326
FlashPoint/MCI Video I/O Settings sub-tab 1366
FlashPoint/MCI Video Settings
procedures 1367
FlashPoint/MCI Video Settings sub-tab . 1364
Floor tracking elevator control mode 676
Fonts-change list font 57
Formats exported 1344
Frame rates-increase during events 966

G

Gates form 487
procedures 488
Gateway readers
addresses 637
reader number 637
General Cardholder Options form 423
General Settings sub-tab 1353
procedures 1356
General System Options form 392
Generate Event Properties Window 1216
Getting started 49
Global APB System/Segment Reset Properties window 1218
Global I/O
alarm monitoring 806
folder 805
linkage failure 807

linkages-how they work 807
overview 805
segmentation 806
Global Linkage form
Global Linkage sub-tab 808
Input Event sub-tab 809
Output Action sub-tab 812
procedures 813
Global Output Devices folder 529
Global Output Server-overview 529
goVision video recorder
add camera input 971
add camera output 974
add recorder 935
overview 917
pre- and post-roll 955
Grant/Deny Popup Properties window ... 1219
Groups folder 777
GSC (iCLASS) smart card format 262
Guard 134
Guard Tour
assign security clearance levels 134
folder 891
overview 891
Guard Tours
form (Cardholders folder) 134
procedures 134

H

Hand geometry
capture hand print templates 1382
functionality 1380
hand print templates 1383
license 1380
permissions 1380
verify hand print templates 1382
Hand Geometry form 1380
Hand print templates
capture 1382
modify 1383
verify 1382
Help menu 68
HID access control (mifare) card format .. 270
HID form
Card Formats sub-tab 624
Connection sub-tab 623
Location sub-tab 621
Overview 620
HID form procedures 625
Hide disabled user accounts 353
High resolution analog video capture 1368
Holidays form 705
procedures 707

I

iCLASS access control smart card format 267
Icon type 908
ID allocation
configure for every badge type 443
configure for specific badge type 325
ID fixed range
procedures (by all badge types) 444
procedures (by badge type) 326
ILS
configure special purpose cards 1511
download commands 1503
introduction 1473
ILS Authorization form 137, 198
ILS badge types 1487
ILS custom encoding 1486
ILS form 677, 681
ILS forms
overview 541
ILS lock reports 1514
ILS locking systems 1491
ILS locks
access control card formats for 1499
calculate maximum cardholders 1504
card formats for 1499
Download Required icons 1503
iCLASS printing and encoding 1512
initialization/download required 1502
OMNIKEY encoders and 16kBit cards 1513
select modes of operation during a timezone 1509
smart card formats 1499
special purpose cards 1511
ILS Mobile Configurator
Communication Server requirement 1506
ILS Offline form 1492
Location sub-tab 1492
Operator sub-tab 1493
Options sub-tab 1496
ILS offline lock 1499
Add Operator dialog 1494
ILS offline lock panels 1498
ILS offline lock processing 1498
ILS offline/wireless holidays 1508
ILS Priority One Events 1523
ILS Priority One Events Form 879
ILS Priority One Events form 681
ILS timezones 1508
ILS Wireless form 1514
Connection sub-tab 1516
Location sub-tab 1515
ILS wireless lock panels 1519
ILS wireless lock processing 1519
ILS wireless locks 1520
configure system options for 1522
ILS Priority One Events 1523
Image
apply chromakey 1346
capture using digital camera 1374
compress 1359

Image capture procedures 1343
Image formats supported 1377
Image Processing window 1349
Image requirements
automatic cropping 1357
Images
export 1344
scan 1371
Import
cardholder data 99
file using Multimedia Capture 1375
fingerprints from PIV card 97
image from an existing file 1376
multi-resolution image file 1376
non-supported image 1376
In Reader 1559
In-Camera Storage 957
camera configuration 957
camera requirements 957
Inclusion group procedures 737
Input Event Configuration form 811
Input Point-Types 1578
Input/Output Local Linkage form 697
procedures 697
Instant arm 1201
Integra lock overview 1482
Integra lock processing 1480
Integra locks
Download Required icons 1503
initialization/download required 1502
overview 1475
Integra Offline form 1475
Connection sub-tab 1477
Location sub-tab 1476
Operators sub-tab 1478
Integra panel overview 1481
Integra timezones 1489
Integra timezones/reader modes 1490
IntelligentAudio Events form 1018
procedures 1020
IntelligentVideo Events form
procedures 1014
IntelligentVideo folder 1009
IntelligentVideo Server form 1010
procedures 1011
Intercom Call Properties window 1220
procedures 1222
Intercom communication 1061
Intercom Devices folder 1061
Intercom Devices form 1062
Intercom Functions form 1069
Intercom Stations form 1067
Intercom Devices form
procedures 1065
Intercom exchange procedures 1065
Intercom Functions form
procedures 1070
Intercom Stations form
procedures 1068
Interior 1201
Interlock
escorts and turnstiles 755
overview 754
Intrusion Detection Configuration Folder
Areas form 1140
Intrusion Detection Configuration folder 1123
Intrusion Panels form
Connection sub-tab 1125
Encryption sub-tab 1128
Location sub-tab 1123
Options sub-tab 1127
procedures 1129
Iris patterns 1392
IrisAccess (iCLASS) card format 279
IrisAccess 3000
capture templates 1395
capture tips 1395
encode access control information . 1396
encode smart cards 1396
enrollment process 1392
functionality 1392
license 1392
permissions 1392
verification process 1393
verify templates 1396
IrisAccess 3000 form 1392
IrisAccess iCAM
encode smart cards 1399
verify templates 1399
IrisAccess iCAM form 1397
ISC Database Download Properties
window 1222
ISC Firmware Download Properties
window 1224
ISO 7811 magnetic track formats 303
Issuance validation 1466
Issue badge
check if badge already issued 1467
IVS form 1010

J

JIS magnetic encoding 1447

K

Keyboard commands 359
Keyboard Wedge Settings window 90
Keypad command readers 641
program 672

L

Lantronix box communication configuration for
receivers 1095
LDVR video recorder
add camera 963
add multiple cameras 938

add recorder 935
LDVR-408 video recorder overview 914
LDVR-444 video recorder overview 915
LDVR-SP video recorder overview 912
LDVR-SP30 video recorder overview 913
Licenses
Bioscrypt applications (V-Smart) 289
Fingerprint (Bioscrypt) 1384
Hand geometry 1380
HID devices 622
iCLASS Access Control application 269
IrisAccess 3000 1392
multimedia capture 1339
SmartID (MIFARE) application 274
Licensing requirements for CMS 1456
Link
camera devices to checkpoints 901
cardholder to a directory account 131
device to a local I/O function list 798
text library entry 499
user account to a directory account .. 351
Link Access Panel form 799
Link Alarm Panel form 800
Link Area form 803
Link Host form 799
Link Reader form 801
Link Summary View window 850
List Builder folder 481
List fonts-change 57
LNL-1000 form
Connection sub-tab 599
Diagnostics sub-tab 604
Encryption sub-tab 605
Location sub-tab 597
Options sub-tab 601
overview 596
procedures 606
LNL-2000 form
Diagnostics sub-tab 592
Encryption sub-tab 593
Location sub-tab 581
Notes sub-tab 593
Options sub-tab 589
overview 581
Primary Connection sub-tab 583
procedures 594
Secondary Connection sub-tab 586
LNL-2210 form
Connection sub-tab 573
Diagnostics sub-tab 577
Encryption sub-tab 578
Location sub-tab 571
Options sub-tab 574
overview 570
procedures 579
LNL-2220 form
Diagnostics sub-tab 566
Encryption sub-tab 567
Location sub-tab 558
Options sub-tab 562
Primary Connection sub-tab 560
procedures 568
LNL-3300 form
Diagnostics sub-tab 553
Encryption sub-tab 554
Location sub-tab 542
Notes sub-tab 554
Options sub-tab 550
Primary Connection sub-tab 544
procedures 555
Secondary Connection sub-tab 547
LNL-500 form
Connection sub-tab 611
Diagnostics sub-tab 616, 617
Encryption sub-tab 617
Location sub-tab 609
Options sub-tab 613
overview 608
procedures 618
LNL-CK 641
LNVR video recorder
add camera 962
add recorder 933
overview 916
security and passwords 925
Load (user or factory) default settings 1344
Load MIB file(s) 1165
Local I/O folder 791
Local I/O Function Lists form
modify mode 792
procedures 796
view mode 792
Log out of the application 58
Logging in
using automatic single sign-on 54
using manual single sign-on 55
with access to all segments 453
without using single sign-on 52
Logical Access form 133, 328, 434
Logical Access menu 68
Lookup a cardholder assigned to an asset 191
Lost badge handling with CMS 1468

M

Magnetic Card Format form
Card Format sub-tab 248
Segment Membership sub-tab 290
Magnetic track formats
ISO 7811 303
non-standard track configurations .. 1445
standard format attributes 1444
Manual crop adjustment
locking 1359
Manual encryption
configure (non-segmented system) .. 415
configure (segmented system) 477

Mask Groups form
fields ... 779
mask group function links ... 782
overview ... 777
view mode ... 778
Mask/Unmask Alarm Input for Group Properties window ... 1229
Mask/Unmask Alarm Input Properties window ... 1228
Mask/Unmask Alarm Mask Group Properties window ... 1231
Mask/Unmask Door Forced Open for Reader Group Properties window ... 1236
Mask/Unmask Door Forced Open Properties window ... 1234
Mask/Unmask Door Held Open for Reader Group Properties window ... 1239
Mask/Unmask Door Held Open Properties window ... 1237
Mask/Unmask Door Properties window . 1233
Masking motion ... 967
Master arm ... 1201
Master Key Entry window
Segments folder ... 476
System Options folder ... 413
Master keys
activate (non-segmented system) ... 416
activate (segmented system) ... 479
export (non-segmented system) ... 416
export (segmented system) ... 478
modify (non-segmented system) ... 416
modify (segmented system) ... 478
Matrix switcher
form ... 1036
overview ... 1035
Matrix switcher type
form ... 1039
procedures ... 1040
Matrix switcher variable designations ... 1044
Maximum cardholder for ILS locks ... 1502
Menus
access control ... 64
additional hardware ... 67
administration ... 62
application ... 60
asset ... 71
cardholder ... 69
edit ... 61
help ... 68
logical access ... 68
monitoring ... 66
video ... 66
view ... 61
window ... 68
Messages form ... 870
MIB files-loading ... 1165
MobileVerify folder ... 485
MobileVerify overview ... 485
Modem Settings form ... 701
Modify
access levels assignments ... 122
action group ... 527
alarm definition record ... 857
alarm priority range ... 863
area (Areas folder) ... 768
asset ... 182
asset classes assignment ... 186
asset group ... 131
audio clip record ... 867
automatic message ... 875
badge record ... 115
badge type ... 312
badges for selected cardholder group 115
card format ... 304
cardholder permission group ... 366, 373
cardholder record ... 103
cardholder's permission to have visitors ... 129
CCTV instruction record ... 869
custom expression ... 299
DataConduIT Device ... 1173
DataConduIT message queue ... 496
DataConduIT Source ... 1171
DataConduIT Sub-Device ... 1175
directory ... 341
entry in a list ... 483
field/page viewing permission group 376
fire device ... 1057
fire input/output ... 1059
fire panel ... 1055
global I/O linkage ... 815
global I/O linkage's segment ... 815
group of cardholder's segments ... 108
hand print templates ... 1383
HID access panel ... 625
holiday ... 708
ILS offline lock panel assignment . 1501
ILS offline lock type ... 1502
ILS wireless lock panel assignment 1522
ILS wireless lock type ... 1522
intrusion panel ... 1130
intrusion panel's segment ... 1130
LNL-1000 access panel ... 607
LNL-2000 access panel ... 595
LNL-2210 access panel ... 580
LNL-2220 access panel ... 568
LNL-3300 access panel ... 556
LNL-500 access panel ... 619
local I/O function list ... 797
lock type ... 1502
matrix switcher ... 1038
matrix switcher type ... 1040
monitor permission group ... 370
monitor zone ... 884
monitoring assignment ... 887
paging device ... 534

panel user group 1146
panel user group's segment 1146
personal safety panel 1080
print setup 316
receiver 1104
receiver account 1108
receiver account group 1112
recipient 537
report 210
scheduled action using the scheduler right-click menu 523
SNMP Agent 1163
SNMP Management Information Base variable 1166
SNMP Manager 1160
system permission group 363
text library entry 499
text record 864
timezone 710
timezone/area assignment 718
timezone/reader assignment 714
transmitter 1085
transmitter input 1088
user information 353
visit record 157
visitor record 106
workstation entry 382
zone 1114
Monitor
ILS wireless lock events 1524
Monitor Permission Groups form
Control Device Groups sub-tab 369
overview 366
Permissions sub-tab 367
permissions tree 368
procedures 370
Monitor Stations form 885
procedures 886
Monitor Zones folder 881
Monitor Zones form
procedures 884
view mode 881
Monitoring menu 66
Monitoring Options folder 907
Motion detection configuration 967
LDVR 967
Motion Detection event
configuration/search dialog 1003
overview 1003
Motion mask applied to camera 967
Motion masking 967
Move the crop window 1358
Move the system tree when it is docked 78
Multi-drop support-virtual matrix switcher
LDVR-408 914
LDVR-444 915
LDVR-SP 913
LDVR-SP30 913
Multimedia Capture
licenses and permissions 1339
procedures 1343
Multimedia Capture module 1339
Multi-resolution image files 1376
Mustering
Muster Reporting form 773
overview 753
procedures 774

N

New Segment wizard 459
NGP Access Panel Configuration . 1527, 1589
Network Settings 1568
NGP Panel Equipment Point 1538
NGP Readers 1549
NGP event message references
sorted by CID code 1585
sorted by SIA code 1582
NGP form
overview 541
NGP transmitted messages 1579
Contact-ID (CID) format 1581
door alarms 1581
SIA Level II format 1580
NGP/CASI Access Panel Configuration
NGP/CASI Form 1527
Non-HID hardware licenses 622
Notes form 682

O

Object segmentation table 1421
Offboard Relays form 1136
procedures 1138
Onboard Relays form 1134
procedures 1135
OPC Connections
folder 1177
procedures 1180
OPC Sources
form 1182
procedures 1183
Open/Close APB Area Properties window 1241
Operator
Integra locks 1478
Other form
Connection sub-tab 628
Location sub-tab 626
Options sub-tab 630
overview 626
procedures 631
Out reader 1561
Overwrite Facial Image Dialog 97

P

Paging Devices form 532
procedures 533

Pan, tilt, and zoom
LDVR-408 914
LDVR-444 915
LDVR-SP 912
LDVR-SP30 913
Panel User Assignment Wizard
Find Person form 1143
Select Person form 1144
Summary form 1145
Panel User Groups form 1142
procedures 1145
Parameter-based events 856
Password
change network video 994
enable/disable strong password enforcement 50
overview 49
standards 50
weak database warning 51
Passwords 57
Pelco "D" protocol 1039
example 1045
message format 1042
standard command set 1043
Perimeter 1201
Perimeter arm 1201
Permission group trees 356
Permission tree keyboard commands 359
Permissions
Bioscrypt 1384
Hand geometry 1380
IrisAccess 3000 1392
modify cardholder and visitors 129
multimedia capture 1339
OpenCapture 1387
Person e-mail fields
modify 450
Person E-mail Fields form 439
Personal safety devices
overview 1073
Personal Safety Devices folder 1073
Personal Safety Devices form
Connection sub-tab 1076
Location sub-tab 1075
procedures 1079
Perspective Correction
configure 1030
Photo capture from live video 1363
Photo form 1340
PIV card
75-bit card format 259
verify fingerprints 97, 1466
Policy for CMS 328
POS devices
hardware setup and configuration .. 1150
licenses required 1150
overview 1149
storing transactions 1150
user permissions required 1150
POS Devices form
Connection sub-tab 1152
Encryption sub-tab 1153
Location sub-tab 1151
procedures 1154
POS Register form 1155
procedures 1156
Precision Access form
Cardholders folder 125
procedures 125, 737
Precision access groups-assign 126
Preview
report 211
Preview a badge 141
Primary segments 1413
Print
badge 141
badge for a visitor 158
report 211, 238
Print Badge(s) window 149
Print Report Options window 237
Printers to encode magentic stripes for ILS 1487
Printing form
procedures 316
Printing/Encoding form 314
Prioritize card formats for reader 1500
Priority form 860
Program reader keypad commands 672
Promote an LNL-1000 access panel to an LNL-2000, 2210, 2220, or 3300 access panel 608
Promote an LNL-2000 access panel to an LNL-2210, 2220, or 3300 access panel 595
Promote an LNL-2210 access panel to an LNL-2220 or 3300 access panel 580
Promote an LNL-2220 access panel to an LNL-3300 access panel 570
Promote an LNL-500 access panel to an LNL-1000, 2000, 2210, 2200, or 3300 619
PTZ Tour Server form 994
Pulse Open Door Group Properties window 1243
Pulse Open Door Properties window 1242

R

Random tour lists 902, 903
Reader form
procedures 642
Reader Mode Group Properties window 1246
Reader Mode Properties window 1245
Reader Reports form 211
overview 211
procedures 214
Readers - keypad command 641
Readers folder 635
Anti-Passback form 666

Aux Inputs form 656
Aux Outputs form 659
Command Programming form 669
Controls form 651
Elevator Hardware form 672
ILS form 677, 681
ILS Priority One Events form 681
Notes form 682
Reader form 635, 643
Settings form 645
Receiver Account Groups form
Account List sub-tab 1111
Details sub-tab 1109
Receiver Account Zone Reports form 233
overview 233
procedures 235
Receiver Accounts form
Details sub-tab 1105
Options sub-tab 1107
procedures 1111
Receiver accounts-overview 1094
Receivers
overview 1093
Receivers folder
Areas form 1115
Event Code Templates form 1118
Receivers form
Connection sub-tab 1100
Encryption sub-tab 1102
Location sub-tab 1097
Options sub-tab 1101
procedures 1103
Recipients form 534
procedures 537
Record
add cardholder 103
add or replace badge 114
add visitor 106
Record archive and restore processes 503
Redundancy
overview 920
Refresh actions 522
Region of Interest
set 1029
Remote Monitor form 974
procedures 976
Remove
access levels from cardholder group 122
event and timezone pairs from an event routing group 890
precision access groups from a badge 126
timezone/area assignment 718
timezone/reader assignment 715
Report Configuration form 206
procedures 210
Report Print Preview window 242
procedures 243
Reports 193, 1401
run a cardholder report 135
run a date/time report 225
run a reader report 214
run a receiver account zone report ... 236
run a visit report from the Visits folder 167
run an alarm acknowledgment report 232
run an alarm panel report 217
run an anti-passback report 221
run an asset report 193
run an event report 229
Reports for ILS locks 1514
Reports form 166
Assets folder 191
Cardholders folder 135
Required encoders for ILS iClass cards . 1512
Required fields by badge type 320
Required Fields form 319
procedures 320
Reset
disabled text color 57
list font 57
toolbars to their default settings 72
Reset Use Limit Properties window 1248
Resistor tables 819
Resize the crop window 1358
Restore records to the database 512
Restoring form 509
Restrict user access to segments 352
Retrieve the most recent search results 183
Retrieve the most recent visit search results 154
Revoke
PKI credentials in CMS 1468
Run 193
Run PTZ Tour Properties window 1250

S

Scan an image 1371
Scan barcodes with wedge scanner 91
Scan images
bypass preview 1372
Scanner Settings sub-tab 1370
procedures 1371
Scanners form
Communications sub-tab 385
Encoding sub-tab 388
General sub-tab 384
Location sub-tab 385
overview 382
procedures 388
Schedule
action 516
automatic guard tour action 906
one-time password change 1206
recurring password change 1206
visits 152

Schedule Report Properties window 1251
Scheduler folder 515
Scheduler form (Guard Tour folder) 905
procedures 906
Scheduler form (Scheduler folder) 515
procedures 516
right-click menu 521
Search
biometric records 127
cardholder records 88
comparison operators 87
for all visits by a selected visitor 152
for all visits for a specific date or time 153
for all visits to a selected cardholder 151
for an asset record 183
for scheduled, active, or finished visits 152
report for specific information 245
Search for users by permissions 354
Search form 354
Search results
configure for visitors 448
configure for visits 448
retrieve recent search results 89
Security clearance levels
assign 134
definition 903
Security form 992
procedures 994
Segment Groups form 479
Segment Membership form 313
Segment Options form 459
procedures 461
Segmentation 806
add new segment wizard 459
add segments 454
advanced 1413
allow other segment users to assign access levels 1418
assigning access levels example 1419
badge types 1416
card formats 1416
cardholders 1417
configure installation for segmentation 462
destination assurance on segmented systems 825
enable segmentation features 463
modify access levels for additional segments 728
modify cardholder segment assignments 108
multiple segment guidelines 1412
Object Segmentation table 1421
overview 1411
primary segments 1413
ramifications and process flow 1420
segment users and all segments users 1412
usage scenarios 1414
visitor 1418
Segments 471, 473
Segments and segment groups 1411
Segments folder 453
Segments form
Cardholders folder 107
procedures 108
Segments form (Segments folder)
Access Levels sub-tab 471
Anti-Passback sub-tab 465
Assets sub-tab 469
Biometrics sub-tab 466
Controller Encryption sub-tab 473
Extended Held Command sub-tab ... 469
Hardware Settings sub-tab 463
procedures 479
Visits sub-tab 470
Select Badge Layout window 308
Select Date(s) window 160
Select Decimal ASCII Code dialog 298
Select Host Wizard-Search form 168
Select Host Wizard-Select form 170
Select Import Source window 176
Select modes of operation for Integra locks during a timezone 1490
Select PTZ Preset Properties window 1255
Select reader modes during a timezone 714, 717, 1509
Select Recipient window 872
Select Time Range window 161
Select Visitor Wizard - Add form 174
Select Visitor Wizard - Search form 171
Select Visitor Wizard - Select form 175
Select Visitor Wizard - Select or Add form 172
Selective cardholder download 829
Set keys
automatic encryption (non-segmented system) 414
automatic encryption (segmented system) 477
manual encryption (non-segmented system) 415
manual encryption (segmented system) 477
Set up
host modem 703
Settings form 645
procedures 651
Setup
install ActivClient 1456
install OnGuard license 1456
OnGuard CMS Client 1456
Show disabled user accounts 353
SIA & Contact-ID message format 1579
SIA Level II message format 1580

Sign in a previously scheduled visit 158
Sign In Visit(s) window 148
Sign out a visit 159
Sign Out Visitor Properties window 1259
Signature capture 1361
Signature Settings sub-tab 1359
procedures 1360
Simple Lists form 481
procedures 483
SLC-5 (SpiderAlert local controller) 1074
Smart card formats
Credential Agent 261
GSC (iCLASS) 262
hid access control (iclass) 267
hid access control (mifare) 270
IrisAccess (iCLASS) 279
SmartID (MIFARE) 272
V-Smart (iCLASS) 286
V-Smart (MIFARE) 286
Smart card formats for ILS locks 1499
SmartID (MIFARE) smart card format 272
SMTP Server Settings form 530
procedures 531
SNMP Agents form 1161
procedures 1162
SNMP Management Information Base form 1163
procedures 1165
SNMP Managers folder 1157
SNMP Managers form 1158
procedures 1159
Sort reader card formats 1500
Special purpose cards overview 1511
Special Two-Man Rule
configuration instructions 1439
configuring the access panels 1440
configuring the areas 1440
configuring the badges 1441
configuring the list builder 1441
configuring the timezone 1442
definitions 1437
overview 1436
special 1-man mode 1437
special 2-man mode 1438
Standard 26-Bit Wiegand card format 258
Standard 75-Bit PIV card format 259
Standard Two-Man Rule
overview 1435
Start an action 521
Status Search form 162
Stop an action 521
Supported image formats table 1377
Surveillance IP Camera(s) Firmware Download Properties window 1262
Synchronize active badges with active visits 445
System Options
ILS form 1485
System Options folder 391
Access Levels form 408
Anti-Passback form 400
Biometrics form 402
Controller Encryption form 410
Hardware Settings form 398
User Command form 404
Visits form 406
Web Applications form 397
System Permission Groups form
overview 361
permissions tree 362
procedures 362
System Settings form 486
procedures 486
System tree 76, 78
System tree procedures 73
System tree-display 73
System-wide visit options
configure 445

T

Tailgate and alarm shunt compatibility 648
Terms used in this document 1473
Text color 57
Text color-change disabled text color 57
Text form 863
Text Library folder 497
Text Library form 498
procedures 498
Threshold settings in the ACS.INI file for dialup panels 632
Timed anti-passback-configure 669
Time-lapse recording
configure with LDVR 968
configure with LNVR and motion detection 968
Timezone/Reader Modes form
procedures 714
view mode 711
Timezones folder 705
Timezones form 708
procedures 710
Timing and alarms 1564
Toolbars 59
how to use 72
Tour Groups form 902
procedures 904
Tours form
Checkpoint Actions sub-tab 893
Checkpoints sub-tab 893
Messages sub-tab 894
Monitoring Stations sub-tab 894
procedures 896
Tour Video sub-tab 895
Transmitter Inputs form 1086
procedures 1088
Transmitters form 1081

procedures 1084
Troubleshoot logging in 57
Two-Man Rule 1435

U

Unassign an asset 191
Unlink
directory account 132
user account from a directory account 352
Upload
ILS lock events 1507
Integra lock events 1484
User accounts
add 350
assign a monitor zone 350
assign access levels 350
delete 353
disable 353
hide disabled user accounts 353
link to a directory account 351
modify 353
restrict access to segments 352
show disabled user accounts 353
unlink from a directory account 352
User Command
non-segmented system 404
User permissions
Dependencies 360
User permissions for global I/O 806
User permissions for logical access 1457
Users folder 343
Users form
Area Access Manager Levels sub-tab 348
Directory Accounts sub-tab 346
General sub-tab 345
Internal Account sub-tab 346
Monitor Zone Assignment sub-tab .. 349
overview 343
Permission Groups sub-tab 347
procedures 349
Replication sub-tab 349
Segment Access sub-tab 348

V

Validate
badge status for issuance 1466
Variables for matrix switchers 1044
Verify
connectivity to CMS 1458
fingerprint (Bioscrypt) templates ... 1386
fingerprints for PIV card 1466
hand print templates 1382
IrisAccess templates 1396
user permissions 1457
Verify fingerprint 97
Verify fingerprint templates 1391
Verify Fingerprint(s) Dialog 96
Video capture
use high resolution for analog capture 1368
Video capture cardholder image 1363
Video Channel Configuration
configure parameters 1033
dialog 1032
open dialog 1031
procedures 1033
Video menu 66
Video Processing form 994, 998
procedures 1006
Video recorder
failover 920
redundancy 920
Video Recorder form
Archiving/Purging sub-tab 927
Connection sub-tab 924, 925
goVision procedures 935
LNVR procedures 933
other recorder procedures 935
procedures 933
add other recorders 935
Recording sub-tab 926
right-click menu 922
Video-change network video password 994
View
action history 522
automatic message 875
current status of an action 522
device-event-alarm links 855
ILS offline lock events 1506
Integra offline lock events 1484
View menu 61
View options change cardholders folder view 89
Visit
right-click menu 146
search capabilities 150
Visit form 159
Visit notification fields configure 449
Visit Notification Fields form 438
Visit options configure system-wide 445
Visit search results 154
Visit Search Results Lists form 437
Visitor
add record 106
configure search results lists 448
find cardholder/visitor associated with a visit 154
print badge for a visitor 158
search for all visits by a selected visitor 152
Visitor form 105
procedures 105
Visitor Search Results Lists form 436
Visitor segmentation 1418

Visits
active 152
add a visit record 154
delete a visit record 158
find cardholder/visitor associated with a visit 154
finished 152
modify a visit record 157
retrieve recent search results 89
retrieve recent visit search results 154
run a visit report from the Visits folder 167
search all visits by selected visitor ... 152
search all visits for specific date or time 153
search all visits to selected cardholder 151
search for active visits 152
search for finished visits 152
search for scheduled visits 152
sign in a previously scheduled visit . 158
sign out a visit 159
synchronize active badges with visits 445
synchronize summary table 446
Visits configure search results lists 448
Visits folder
field table 147
procedures 150
Visits form 431
Cardholders folder 128
procedures 129
Visonic bus device-procedures 688
V-Smart (iCLASS) smart card formats 286
V-Smart (MIFARE) smart card formats ... 286

W

WDM Video Settings sub-tab 1361
procedures 1362
Weak database password warning 51
Wedge scanner
add a badge 90
configure 94
scanning barcodes 91
search for a badge 90
Wedge Settings window 90
Wiegand card format
75-bit PIV 259
standard 26-bit 258, 259
Wiegand Card Format form
Card Format sub-tab 252
procedures 257
Segment Membership sub-tab 290
Wiegand Card Format form (ILS)
Card Format sub-tab 254
Window menu 68
Wizards 60
add new segment 459
Application wizards 78
select host wizard (Search form) 168
select host wizard (select form) 170
select visitor wizard (Add form) 174
select visitor wizard (select or add form) 172
Workstations 377
Workstations form
Activity Printer sub-tab 378
CCTV Controller sub-tab 379
Gate Configuration sub-tab 381
overview 377
procedures 381
Video Capture Device sub-tab 380

Z

Zones form
modify mode 1113
procedures 1114
view mode 1112
Zones form (Intrusion Detection Configuration folder) 1132
procedures 1133

Lenel Systems International, Inc.
1212 Pittsford-Victor Road
Pittsford, New York 14534 USA
Tel 585.248.9720 Fax 585.248.9185
www.lenel.com
docfeedback@lenel.com