Alarm Monitoring User Guide
Lenel OnGuard® 2013 Alarm Monitoring User Guide, product version 6.6
This guide is part 1 of a 2-document suite, item number DOC-201, revision 3.009, July 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 Alarm Monitoring

- Conventions Used in this Documentation
- How this Document is Organized
- Getting Started
  - Passwords
  - Enable/Disable Strong Password Enforcement
  - Error Messages
  - Accounts
  - Log In
- Single Sign-On
  - Directory Accounts
  - Automatic and Manual Single Sign-On
  - Configure Single Sign-On
  - Log In Using Automatic Single Sign-On
  - Log In Using Manual Single Sign-On
- Troubleshoot Logging In
- Assigning Directory and Internal Accounts to the User
  - Switch Log On
  - Log Out of the Application
  - Exit the Application

Chapter 2 - Main Alarm Monitoring Window

- Menus and Toolbars
  - File menu
  - Edit menu
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>View menu</td>
<td>33</td>
</tr>
<tr>
<td>Trace menu</td>
<td>35</td>
</tr>
<tr>
<td>Configure menu</td>
<td>36</td>
</tr>
<tr>
<td>Control menu</td>
<td>36</td>
</tr>
<tr>
<td>Control menu - “Current Device” sub-menu</td>
<td>37</td>
</tr>
<tr>
<td>Options menu</td>
<td>39</td>
</tr>
<tr>
<td>Window menu</td>
<td>42</td>
</tr>
<tr>
<td>Help menu</td>
<td>42</td>
</tr>
<tr>
<td>Cardholder menu</td>
<td>43</td>
</tr>
<tr>
<td>Cardholder menu - Bulk sub-menu</td>
<td>44</td>
</tr>
<tr>
<td>Asset menu</td>
<td>45</td>
</tr>
<tr>
<td>How to Use the Toolbars</td>
<td>46</td>
</tr>
<tr>
<td>Alarm Monitoring Status Bar</td>
<td>46</td>
</tr>
</tbody>
</table>

## System Administrator Procedures

### CHAPTER 3 System Administrator Procedures

- Administrative Procedures Checklist                                    | 49   |
- Access Control Procedures Checklist                                     | 50   |
- Intrusion Detection Alarm Definitions                                   | 51   |
- Alarm Monitoring Operator Procedures                                     | 51   |
- Intrusion Detection Device Statuses                                     | 51   |
- Monitoring Procedures Checklist                                          | 52   |
- Video Procedures Checklist                                              | 52   |

## Operator Procedures

### CHAPTER 4 Set Alarm Monitoring Display Options

- System Status Options Window                                            | 55   |
- Display Option Procedures                                               | 57   |
  - Select Event Types to Monitor                                         | 57   |
  - Select Column Configuration                                           | 58   |
  - Set Automatic Display Options                                         | 59   |
  - Toggle Window Display Modes                                           | 59   |
  - Display Multiple Windows in the Main Window                           | 60   |
  - Select Hardware View Options                                          | 61   |

### CHAPTER 5 Monitor Devices

- System Status Window                                                    | 63   |
- Device Groups Window                                                     | 64   |
- Device Group Test Mode Window                                           | 65   |
# Table of Contents

- **Device Group Icons** .................................................. 66
- **Hardware Device Icons** ............................................. 66
- **Device Status** .......................................................... 68
  - **Runaway Devices** .................................................. 68
  - **Offline Hardware Devices** ...................................... 68
- **Procedures for Monitoring Devices** ................................. 70
  - **Update the Hardware Status** .................................. 70
  - **Perform a Device Test** ....................................... 70
  - **Locate or Search for a Device** .................................. 71
  - **View the Last Connection Time for Dialup Panels** .......... 71
  - **Download the OnGuard Database or Firmware** ............... 71
  - **View the Controller Properties** .................................. 72
  - **View Notes** ............................................................ 72

## CHAPTER 6

**Trace Alarms and Events** ............................................. 75

- **Trace Configuration Window Overview** .......................... 75
- **Trace Configuration Window** ...................................... 76
- **Procedure for Tracing** ............................................. 77
  - **Trace Alarms and Events** ....................................... 77

## CHAPTER 7

**Video Monitoring** ..................................................... 79

- **Video Monitoring Window** ......................................... 80
- **Video Monitoring Window Procedures** ........................... 80
  - **Video Tours** ..................................................... 80
  - **Video Failover Status Indicators** .............................. 81
- **Video Monitoring Features** ......................................... 82
  - **Buffering Streaming Video** ..................................... 82
  - **Browser-based VideoViewer** ...................................... 83
  - **Camera Lookup** ................................................... 83
  - **Two-way Audio** .................................................. 84
- **Video Monitoring Procedures** ....................................... 86
  - **Launch Video (Live/Recorded) From a Camera** ............... 86
  - **Launch Video From a Specific Source** .......................... 86
  - **Monitor Video of a Specific Camera** ........................... 87
  - **Send Video** .......................................................... 87
- **Event Configuration/Search Dialog** ................................ 88
  - **Event Configuration/Search Dialog Menu Options** .......... 90
  - **Event Configuration/Search Dialog Fields** ................... 91
- **Event Configuration/Search Dialog Procedures** ................. 93
  - **Open the Event Configuration/Search Dialog** .................. 93
  - **Configure Event Properties** ................................... 94
  - **Set Region of Interest** ......................................... 95
  - **Video Search Performance Requirements** ...................... 96
  - **Search Video/Audio** ............................................. 96
  - **View Search Results** ............................................. 97
- **Video Channel Configuration Dialog** .............................. 97
  - **Open the Video Channel Configuration Dialog** ............... 98
CHAPTER 9  Video Verification ................................. 133

Video Verification Configuration Dialog .................... 134
Digital Video Verification ..................................... 134
  Set Up Digital Video Verification .......................... 135
Standard Video Verification ................................ 135
Standard Video Verification Procedures ................. 137
  Add or Remove Readers .................................. 137
  Display the Cardholder Photo and Live Video ....... 137
## Table of Contents

Delete an Alarm in the Video Verification Window ........................................... 137

### CHAPTER 10 Cardholder Verification ............................................................. 139
Cardholder Verification Window ....................................................................... 140
Set up Cardholder Verification ....................................................................... 140

### CHAPTER 11 Control Devices and Areas ...................................................... 141
Grant/Deny Pop-up Window ........................................................................... 141
Grant/Deny Pop-up Window Procedures ......................................................... 142
    Grant or Deny Access ........................................................................... 142
Right-click Options to Control Devices and Areas ......................................... 142
    General Right-click Options .................................................................. 143
    Monitor Zone Right-click Options ....................................................... 143
    Access Panel and Alarm Panel Right-click Options ........................... 143
    Intrusion Area Right-click Options ..................................................... 144
    Intrusion Panel Right-click Options .................................................... 144
    Intercom Right-click Options ............................................................... 145
    Intrusion Door Right-click Options ..................................................... 145
    Intrusion Relay Right-click Options ..................................................... 145
    Intrusion Zone Right-click Options ..................................................... 146
    Reader Right-click Options .................................................................. 146
    Reader Group Right-click Options ....................................................... 146
    Alarm Mask Group Right-click Options ............................................... 146
    Intrusion Mask Group Right-click Options ......................................... 147
    Function List Right-click Options ......................................................... 147
    Action Group Right-click Options ....................................................... 147
    Anti-Passback Area Right-click Options ............................................... 147
    Guard Tour Right-click Options ............................................................ 148
    Remote Monitor Right-click options ..................................................... 148
    Remote Monitor Video Cell Right-click Options ................................. 148
    Elevator Terminal Right-click Options .................................................. 148
Single and Double Left-click Mode ................................................................. 149
    Activate Single or Double Left-click Mode ......................................... 149
    Select a Device in Single or Double Left-click Mode .......................... 150
    Execute a Command in Single or Double Left-click Mode ................. 150

### CHAPTER 12 Monitor Alarms ................................................................. 151
Alarm Icons .................................................................................................. 151
Pending Alarms Window .............................................................................. 152
Procedure for Monitoring Alarms ................................................................. 153
    Sort Alarms ......................................................................................... 153

### CHAPTER 13 Acknowledge Alarms ............................................................. 157
Alarm Acknowledgment Window .................................................................... 157
Table of Contents

CHAPTER 14 Muster Mode ..................................................... 165

Overview of Hazardous/Safe Locations .................................. 165
  Hard APB in Hazardous Locations .................................. 165
  Soft APB in Safe Locations .......................................... 166
  Enable Global APB ................................................... 166
Muster Mode Procedures .................................................... 170
  Initiate Muster Mode .................................................. 170
  Reset Muster Mode ................................................... 171
Reports ................................................................. 171
  Run Muster and Occupancy Reports ................................ 172
Moving Badges ............................................................... 172
  Move All Badges from an Area ........................................ 172
  Move a Single Badge from an Area ................................... 173

Advanced Operator Procedures ............................................ 175

CHAPTER 15 Cardholders Folder ............................................. 177

Cardholders Folder Fields .................................................. 178
Cardholders Folder Procedures ............................................ 181
  Cardholder Search Capabilities ...................................... 181
  Search for a Cardholder Record ...................................... 182
  Retrieve the Most Recent Search Results .......................... 183
  Change the Cardholders Folder View Options ...................... 183
Keyboard Wedge Settings Window ......................................... 184
  CAC Barcodes .......................................................... 185
  Scanning Barcodes with a Wedge Scanner .......................... 185
Keyboard Wedge Settings Window Procedures .......................... 188
  Configure a Wedge Scanner .......................................... 188
Verify Fingerprint(s) Dialog ................................................ 190
  Fingerprint Verification with PIV Cards ............................ 190
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Fingerprint(s) Dialog Procedures</td>
<td>191</td>
</tr>
<tr>
<td>Verify Fingerprints from a PIV Card</td>
<td>191</td>
</tr>
<tr>
<td>Import Fingerprints from a PIV Card</td>
<td>191</td>
</tr>
<tr>
<td>Overwrite Facial Image Dialog</td>
<td>191</td>
</tr>
<tr>
<td>Overwrite Facial Image Dialog Procedure</td>
<td>192</td>
</tr>
<tr>
<td>Cardholder Form</td>
<td>192</td>
</tr>
<tr>
<td>Import Cardholder/Visitor Data</td>
<td>193</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>193</td>
</tr>
<tr>
<td>Corex Business Card Scanner</td>
<td>194</td>
</tr>
<tr>
<td>GSC (iCLASS) Card</td>
<td>195</td>
</tr>
<tr>
<td>ID Scan</td>
<td>195</td>
</tr>
<tr>
<td>ID-Check Terminal</td>
<td>195</td>
</tr>
<tr>
<td>PIV Card</td>
<td>196</td>
</tr>
<tr>
<td>TWIC Card</td>
<td>196</td>
</tr>
<tr>
<td>Import Cardholder Data</td>
<td>196</td>
</tr>
<tr>
<td>Cardholder Form Procedures</td>
<td>197</td>
</tr>
<tr>
<td>Add a Cardholder Record</td>
<td>197</td>
</tr>
<tr>
<td>Modify a Cardholder Record</td>
<td>197</td>
</tr>
<tr>
<td>Delete a Cardholder Record</td>
<td>198</td>
</tr>
<tr>
<td>Delete a Selected Group of Cardholder Records</td>
<td>198</td>
</tr>
<tr>
<td>Destroy all Cardholder Data</td>
<td>198</td>
</tr>
<tr>
<td>Visitor Form</td>
<td>199</td>
</tr>
<tr>
<td>Visitor Form Procedures</td>
<td>199</td>
</tr>
<tr>
<td>Import Visitor Data</td>
<td>200</td>
</tr>
<tr>
<td>Add a Visitor Record</td>
<td>200</td>
</tr>
<tr>
<td>Modify a Visitor Record</td>
<td>200</td>
</tr>
<tr>
<td>Delete a Visitor Record</td>
<td>201</td>
</tr>
<tr>
<td>Segments Form</td>
<td>201</td>
</tr>
<tr>
<td>Segments Form Procedures</td>
<td>202</td>
</tr>
<tr>
<td>Modify a Cardholder’s Segment Assignment</td>
<td>202</td>
</tr>
<tr>
<td>Change a Group of Cardholder’s Segments</td>
<td>202</td>
</tr>
<tr>
<td>Badge Form</td>
<td>203</td>
</tr>
<tr>
<td>Badge Form Procedures</td>
<td>208</td>
</tr>
<tr>
<td>Add or Replace a Badge Record</td>
<td>208</td>
</tr>
<tr>
<td>Modify a Badge Record</td>
<td>209</td>
</tr>
<tr>
<td>Modify Badges for a Selected Group of Cardholders</td>
<td>209</td>
</tr>
<tr>
<td>Encoding Prerequisites</td>
<td>210</td>
</tr>
<tr>
<td>Encode a Badge</td>
<td>211</td>
</tr>
<tr>
<td>Delete a Badge</td>
<td>211</td>
</tr>
<tr>
<td>Access Levels Form</td>
<td>211</td>
</tr>
<tr>
<td>Access Levels Form Procedures</td>
<td>213</td>
</tr>
<tr>
<td>Assign Access Levels to a Badge</td>
<td>213</td>
</tr>
<tr>
<td>Assign Intrusion Authority to the Cardholder</td>
<td>214</td>
</tr>
<tr>
<td>Assign Activation and Deactivation Dates to Access Levels</td>
<td>214</td>
</tr>
<tr>
<td>Assign Access Levels to a Selected Group of Cardholders</td>
<td>216</td>
</tr>
<tr>
<td>Remove Access Levels From a Selected Group of Cardholders</td>
<td>217</td>
</tr>
<tr>
<td>Modify Access Levels Assignments</td>
<td>217</td>
</tr>
<tr>
<td>NGP User Form</td>
<td>218</td>
</tr>
<tr>
<td>NGP User Form Procedures</td>
<td>219</td>
</tr>
</tbody>
</table>
CHAPTER 16 Badge Print Preview Window ........................................ 233
  Badge Printing Form .......................................................... 234
  Badge Print Preview Window Procedures .................................. 235
    Preview and Print a Badge ................................................. 235

CHAPTER 17 Visits Folder ......................................................... 239
  Visit Right-Click Menu ...................................................... 240
    Menu Options ............................................................... 240
  Visits Folder Fields .......................................................... 241
    Sign In Visit(s) Window .................................................. 242
    Print Badge(s) Window ................................................... 243
  Visits Folder Procedures .................................................... 244
    Visit Search Capabilities ................................................ 244
    Search for All Visits to a Selected Cardholder ....................... 245

Device Owner Form .............................................................. 219
Device Owner Form Procedures .............................................. 219
  Assign a Cardholder to Own a Device ................................... 219
Precision Access Form .......................................................... 219
Precision Access Form Procedures ......................................... 220
  Assign Precision Access Groups to a Badge ........................... 220
  Remove Precision Access Groups From a Badge ....................... 221
Biometrics Form ................................................................. 221
Biometrics Form Procedures .................................................. 222
  Search for a Cardholder’s Biometric Record ........................... 222
Visits Form ........................................................................... 222
Visits Form Procedures ......................................................... 223
  Modify a Cardholder’s Permission to Have Visitors .................. 223
Assets Form .......................................................................... 224
Assets Form Procedures .......................................................... 225
  Assign an Asset to a Cardholder .......................................... 225
  Unassign an Asset ............................................................. 225
  Modify the Asset Group ........................................................ 225
Directory Accounts Form .......................................................... 225
Directory Accounts Form Procedures ........................................ 226
  Link a Cardholder to a Directory Account ............................... 226
  Unlink a Directory Account .................................................. 227
Guard Tours Form .................................................................... 227
Guard Tours Form Procedures .................................................. 228
  Assign Guard Tour Security Clearance Levels to a Cardholder ...... 228
Reports Form .......................................................................... 229
Reports Form Procedures .......................................................... 229
  Run a Cardholder Report ..................................................... 229
ILS Authorization Form ............................................................. 230
ILS Authorization Form Procedures ............................................ 231

Device Owner Form Procedures .............................................. 219
  Assign a Cardholder to Own a Device ................................... 219
Precision Access Form Procedures ......................................... 220
  Assign Precision Access Groups to a Badge ........................... 220
  Remove Precision Access Groups From a Badge ....................... 221
Biometrics Form Procedures .................................................. 222
  Search for a Cardholder’s Biometric Record ........................... 222
Visits Form Procedures ......................................................... 223
  Modify a Cardholder’s Permission to Have Visitors .................. 223
Assets Form Procedures .......................................................... 225
  Assign an Asset to a Cardholder .......................................... 225
  Unassign an Asset ............................................................. 225
  Modify the Asset Group ........................................................ 225
Directory Accounts Form Procedures ........................................ 226
  Link a Cardholder to a Directory Account ............................... 226
  Unlink a Directory Account .................................................. 227
Guard Tours Form Procedures .................................................. 228
  Assign Guard Tour Security Clearance Levels to a Cardholder ...... 228
Reports Form Procedures .......................................................... 229
  Run a Cardholder Report ..................................................... 229
ILS Authorization Form Procedures ............................................ 231
# CHAPTER 18 Assets Folder

**Assets Folder** .................................................. 271

**Assets Form** .................................................. 272
  - **Asset Types Form** ......................................... 274
  - **Subtypes Form** ............................................. 275

**Assets Form Procedures** ..................................... 275
  - **Add an Asset** ............................................... 276
  - **Modify an Asset** ......................................... 276
  - **Delete an Asset** .......................................... 276
  - **Assign a Cardholder to an Asset** ....................... 276
  - **Search for an Asset Record** ........................... 277
  - **Retrieve the Most Recent Search Results** ........... 277
  - **Add an Asset Type/Subtype** ............................ 277

**Asset Classes Form** .......................................... 278

**Asset Classes Form Procedures** ........................... 281
  - **Assign Classes to an Asset** ........................... 281
  - **Modify an Asset Classes Assignment** ................. 281
  - **Add Asset Groups and Classes** ....................... 281
  - **Modify Asset Groups and Classes** .................... 282

**Search for All Visits by a Selected Visitor** ............... 246
**Search for Scheduled, Active or Finished Visits** .......... 246
**Search for All Visits for a Specific Date or Time** ........ 247
**Retrieve the Most Recent Visit Search Results** ........... 248
**Find a Cardholder or Visitor Associated with a Visit** ..... 248
**Add a Visit Record** .......................................... 248
**Modify a Visit Record** ...................................... 251
**Delete a Visit Record** ...................................... 252
**Print a Visitor Badge** ....................................... 252
**Sign in a Previously Scheduled Visit and Print a Badge** .. 252
**Sign Out a Visit** ............................................. 253

**Visit Form** ................................................... 254
  - **Select Date(s) Window** .................................. 255
  - **Select Time Range Window** ............................. 255

**Status Search Form** .......................................... 256

**Details Form** ................................................ 258

**E-mail Form** .................................................. 258
  - **Add Recipient Window** .................................. 260

**Reports Form** ................................................ 261

**Reports Form Procedures** .................................. 261
  - **Run a Visit Report from the Visits Folder** ........... 262

**Select Host Wizard: Search Form** .......................... 263
**Select Host Wizard: Select Form** .......................... 264

**Select Visitor Wizard: Search Form** ....................... 265
**Select Visitor Wizard: Select or Add Form** ............... 266
**Select Visitor Wizard: Add Form** .......................... 268
**Select Visitor Wizard: Select Form** ....................... 269
  - **Select Import Source Window** ......................... 270

**Search for All Visits by a Selected Visitor** ............... 246
**Search for Scheduled, Active or Finished Visits** .......... 246
**Search for All Visits for a Specific Date or Time** ........ 247
**Retrieve the Most Recent Visit Search Results** ........... 248
**Find a Cardholder or Visitor Associated with a Visit** ..... 248
**Add a Visit Record** .......................................... 248
**Modify a Visit Record** ...................................... 251
**Delete a Visit Record** ...................................... 252
**Print a Visitor Badge** ....................................... 252
**Sign in a Previously Scheduled Visit and Print a Badge** .. 252
**Sign Out a Visit** ............................................. 253
## Table of Contents

**CHAPTER 19**  
Report Configuration Form  ............................................. 290  
Report View Filter Window .............................................. 291  
Report Configuration Form Procedures ................................ 294  
  Add a Report ............................................................. 294  
  Modify a Report ......................................................... 294  
  Delete a Report .......................................................... 295  
  Filter the Report View .................................................. 295  
  Preview and Print a Report ............................................ 295  
Reader Reports Form ....................................................... 295  
Reader Reports Form Procedures .......................................... 298  
  Run a Reader Report ..................................................... 298  
Alarm Panel Reports Form .................................................. 299  
Alarm Panel Reports Form Procedures ..................................... 301  
  Run an Alarm Panel Report ............................................ 301  
Anti-Passback Reports Form ............................................... 302  
Anti-Passback Reports Form Procedures .................................... 305  
  Run an Anti-Passback Report ........................................... 305  
Date/Time Reports Form .................................................... 306  
Date/Time Reports Form Procedures ....................................... 309  
  Run a Date/Time Report ................................................ 309  
Event Reports Form ........................................................ 310  
Event Reports Form Procedures ........................................... 313  
  Run an Event Report ..................................................... 313  
Alarm Acknowledgment Reports Form ...................................... 313  
Alarm Acknowledgment Reports Form Procedures .......................... 316  
  Run an Alarm Acknowledgment Report ................................ 316  
Receiver Account Zone Reports Form ..................................... 317  
Receiver Account Zone Reports Form Procedures ......................... 319  
  Run a Receiver Account Zone Report .................................. 320

**CHAPTER 20**  
Print Report Options Window .............................................. 321  
Print Report Options Window .............................................. 321  
  Print a Report ............................................................. 322
CHAPTER 21 Report Print Preview Window ........................................ 325
  Report Print Preview Window ........................................ 325
  Report Print Preview Window Procedures ........................... 327
    Preview and Print a Report ...................................... 327
    Search a Report for Specific Information ..................... 328

CHAPTER 22 Guard Tour ....................................................... 329
  Start Guard Tour Form .................................................. 330
  Guard Tour Live Tracking Form ...................................... 331
  Guard Tour Form Procedures ......................................... 332
    Launch a Guard Tour ............................................... 332
    Schedule an Automatic Guard Tour Action .................... 333
    Respond to an Automatic Guard Tour ......................... 334
    View a Guard Tour .................................................. 334
  Checkpoint Status and Events Diagram .......................... 335

CHAPTER 23 Scheduler Folder ............................................... 337
  Scheduler Form .......................................................... 337
  Scheduler Form Procedures .......................................... 338
    Add and Schedule an Action ..................................... 338
    Display the Scheduler Right-Click Menu ....................... 343
    Add and Schedule an Action Using the Scheduler Right-Click Menu ........................................... 343
    Start an Action ...................................................... 343
    Stop an Action ........................................................ 343
    View Action History ................................................ 344
    View the Current Status of an Action ......................... 344
    Refresh an Action .................................................... 344
    Refresh all Actions ................................................. 344
    Delete a Scheduled Action using the Scheduler Right-Click Menu ........................................... 345
    Modify a Scheduled Action using the Scheduler Right-Click Menu ........................................... 345

Appendices ................................................................. 347

APPENDIX A Actions ......................................................... 349
  NGP Actions ............................................................... 349
  General Actions Procedures ......................................... 350
    Specify the Number of Simultaneous Actions ................. 350
    Open an Action Properties Window ............................. 350
  Action Group Properties Window ................................ 352
  Action Group Properties Window Procedures .................. 353
    Add an Action Group ............................................... 353
  Action History/Guard Tour Event Purging Properties Window ........................................... 354
### Table of Contents

- Action History/Guard Tour Event Purging Properties Window Procedures .......................................................... 355
  - Add an Action History/Guard Tour Event Purging Action .................................................................................. 355
- Archive/Purge Database Properties Window ........................................................................................................ 355
  - Add an Archive/Purge Database Action .............................................................................................................. 356
- Arm/Disarm Area Properties Window ..................................................................................................................... 356
  - Add an Arm/Disarm Area Action ........................................................................................................................ 358
- Automatic Guard Tour Properties Window .............................................................................................................. 358
  - Add an Automatic Guard Tour Action ................................................................................................................ 360
  - Change Network Video Password Properties Window ......................................................................................... 360
  - Change the Network Video Password ................................................................................................................. 362
  - Schedule a One-Time Password Change ............................................................................................................ 362
  - Schedule a Recurring Password Change ............................................................................................................... 362
- Deactivate Badge Properties Window ...................................................................................................................... 363
  - Add a Deactivate Badge Action .......................................................................................................................... 364
- Device Output Properties Window ............................................................................................................................. 364
  - Add a Device Output Action .................................................................................................................................. 365
- Device Output Group Properties Window ................................................................................................................ 366
  - Add a Device Output Group Action ....................................................................................................................... 367
- Elevator Terminal Allowed Floors Properties Window .......................................................................................... 367
  - Add an Elevator Terminal Allowed Floors Action ............................................................................................... 368
- Elevator Terminal Mode Properties Window ........................................................................................................ 369
  - Add an Elevator Terminal Mode Action .............................................................................................................. 369
- Execute Function List Properties Window ............................................................................................................... 370
  - Add an Execute Function List Action .................................................................................................................... 371
- Generate Event Properties Window .......................................................................................................................... 371
- Global APB System/Segment Reset Properties Window .......................................................................................... 372
  - Add a Global APB System/Segment Reset Action ............................................................................................... 373
- ISC Database Download Properties Window ............................................................................................................ 374
  - Add an ISC Database Download Action .............................................................................................................. 375
- ISC Firmware Download Properties Window .......................................................................................................... 375
  - Add an ISC Firmware Download Action ................................................................................................................ 376
- ISC Database Download Properties Window Procedures ........................................................................................ 375
- ISC Database Download Properties Window Procedures ........................................................................................ 376
- ISC Database Download Properties Window Procedures ........................................................................................ 376
Table of Contents

Moving Badges for APB Areas Properties Window .................................................. 376
Moving Badges for APB Areas Properties Window Procedures .................................. 377
   Add a Moving Badges for APB Areas Action ....................................................... 377
Muster Mode Initiation Properties Window ............................................................. 378
Muster Mode Initiation Properties Window Procedures .......................................... 378
   Add a Muster Mode Initiation Action ................................................................ 379
Mask/Unmask Alarm Input Properties Window ......................................................... 379
Mask/Unmask Alarm Input Properties Window Procedures ...................................... 380
   Add a Mask/Unmask Alarm Input Action ............................................................ 380
Mask/Unmask Alarm Input for Group Properties Window ........................................ 380
Mask/Unmask Alarm Input for Group Properties Window Procedures .................... 382
   Add a Mask/Unmask Alarm Input for Group Action ........................................... 382
Mask (Disarm)/Unmask (Arm) Mask Group Properties Window .............................. 382
Mask (Disarm) / Unmask (Arm) Mask Group Properties Window Procedures .......... 383
   Add a Mask (Disarm)/Unmask (Arm) Mask Group Action .................................. 383
Mask/Unmask Door Properties Window .................................................................. 384
Mask/Unmask Door Properties Window Procedures ............................................... 385
   Add a Mask/Unmask Door Action ..................................................................... 385
Mask/Unmask Door Forced Open Properties Window ............................................... 385
Mask/Unmask Door Forced Open Properties Window Procedures .......................... 386
   Add a Mask/Unmask Door Forced Open Action .................................................. 386
Mask/Unmask Door Forced Open for Reader Group Properties Window .................. 387
Mask/Unmask Door Forced Open for Reader Group Properties Window Procedures .... 388
   Add a Mask/Unmask Door Forced Open for Reader Group Action ...................... 388
Mask/Unmask Door Held Open Properties Window ............................................... 388
Mask/Unmask Door Held Open Properties Window Procedures ............................ 389
   Add a Mask/Unmask Door Held Open Action ..................................................... 389
Mask/Unmask Door Held Open for Reader Group Properties Window .................... 390
Mask/Unmask Door Held Open for Reader Group Properties Window Procedures .... 391
   Add a Mask/Unmask Door Held Open for Reader Group Action ......................... 391
Click this button to display online help for this window. Pulse Open Door Properties Window .392
Pulse Open Door Properties Window Procedures .................................................... 393
   Add a Pulse Open Door Action ......................................................................... 393
Pulse Open Door Group Properties Window ........................................................... 393
Pulse Open Door Group Properties Window Procedures ......................................... 394
   Add a Pulse Open Door Group Action ............................................................... 394
Reader Mode Properties Window .............................................................................. 394
Reader Mode Properties Window Procedures ........................................................ 396
   Add a Reader Mode Action ............................................................................... 396
Reader Mode Group Properties Window .................................................................. 396
Reader Mode Group Properties Window Procedures .............................................. 398
   Add a Reader Mode Group Action ................................................................... 398
Reset Use Limit Properties Window ....................................................................... 398
Reset Use Limit Properties Window Procedures .................................................... 400
   Add a Reset Use Limit Action ......................................................................... 400
Run PTZ Tour Properties Window .......................................................................... 400
### APPENDIX B

**Alarm/Event Descriptions** .................................. 413

NGP Alarm/Event Descriptions .................................. 479

### APPENDIX C

**Reports** .......................................................... 487

Description of Reports ........................................... 487
Deliver Live Video to Alarm Monitoring Using IP Multicast Protocol .... 499

LNVR Network Setup Window ..................................... 500
  - Client Network Settings Form ................................ 500
  - Recorder Network Settings Form ............................... 501
  - IVS Network Settings Form .................................... 502

LNVR Network Setup Configurations ................................ 502
  - Configure Recorder for IP Multicast ......................... 502
  - Configure Client for IP Multicast ........................... 503
  - Configure Router for IP Multicast ............................ 503
  - Configure Firewall for IP Multicast ......................... 503

Video Export Dialog .............................................. 507

Customize Overlay Information Dialog .............................. 508

Video Conversion Procedures ..................................... 509
  - Export Video to a File ....................................... 509
  - Convert and Export Video ................................... 510
  - Play Exported Video Clip Using Windows Media Player ........ 511
  - Authenticate a Video File with Watermarking ................. 511

Audio Level ......................................................... 513
Table of Contents

Event Properties .................................................................................................................. 513
High Pitch Sounds .............................................................................................................. 513
  Event Properties ............................................................................................................. 513
Impact Sounds .................................................................................................................... 514
  Event Properties ............................................................................................................. 514
Unclassified Sounds ........................................................................................................... 514
  Event Properties ............................................................................................................. 514

APPENDIX G Lenel ILS (Integrated Locking Solutions) ...................................................... 515
Offline Locks ...................................................................................................................... 515
  Wireless Locks .............................................................................................................. 515
ILS Offline and ILS Integra Locks ..................................................................................... 516
  Retrieve Events from an ILS Offline Lock ...................................................................... 516
  Retrieve Events from an ILS Integra Lock ..................................................................... 516
ILS Wireless Locks ........................................................................................................... 517
  Retrieve Events from Wireless Locks ............................................................................ 517
  Download ILS Wireless Locks ...................................................................................... 517
  Monitor ILS Wireless Lock Events .............................................................................. 517
  View Wireless Lock Status ............................................................................................ 518
  Change Reader Access Modes ...................................................................................... 519
  Secure/Unsecure All Locks from a Reader Device Group .............................................. 520
Wireless Diagnostics Dialog .............................................................................................. 520
  View Wireless Diagnostics Information ....................................................................... 521
ILS Wireless Firmware ....................................................................................................... 521
  Download Wireless Gateway Firmware ......................................................................... 522
  Download ILS Wireless Lock Firmware ...................................................................... 522
Introduction
CHAPTER 1

Introduction to Alarm Monitoring

The Alarm Monitoring application displays information about individual alarms and events as they occur. Operators can acknowledge alarms and manually change the status of devices as well as monitor video and launch Guard Tours.

With the correct permissions, Operators can also perform a variety of administrative tasks such as adding, modifying, deleting and tracking cardholders, visitors and assets as well as print badges.

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]`.

How this Document is Organized

The Alarm Monitoring User Guide is divided into three sections: the System Administrator Procedures section, the Operators section and the Advanced Operator Procedures section.

The System Administrator section outlines the steps involved in setting up an Alarm Monitoring station. Most of the procedures in these chapters reference other manuals because they cannot be performed in the Alarm Monitoring application.

The Operator Procedures section focuses on procedures to monitor alarms, monitor video, trace devices and execute commands.
The Advanced Operator Procedures section covers the administrative procedures operators can perform in Alarm Monitoring. For example, adding cardholders or visitors, printing badges, adding assets to the database and assigning assets to cardholders.

Note: Depending on the workflow of your company, some of the procedures covered in this section may be considered System Administrator procedures.

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 25.

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:
Getting Started

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].

**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 22.

<table>
<thead>
<tr>
<th>Warning message</th>
<th>Password to correct</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Database</td>
</tr>
<tr>
<td>Your password cannot be blank. Please enter a password.</td>
<td>User</td>
</tr>
<tr>
<td>User password violations: Passwords cannot be the same as the user name.</td>
<td>User</td>
</tr>
<tr>
<td>Your password is a keyword that is not allowed.</td>
<td>User</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>User name</th>
<th>Password</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sa</td>
<td>sa</td>
<td>system account</td>
</tr>
<tr>
<td>admin</td>
<td></td>
<td>sample</td>
</tr>
<tr>
<td>user</td>
<td></td>
<td>sample</td>
</tr>
<tr>
<td>badge</td>
<td></td>
<td>sample</td>
</tr>
</tbody>
</table>

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 25. To log in using single sign-on, refer to Configure Single Sign-On on page 26.

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].
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].

5. If you are prompted to select a monitor zone:
   a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.
   b. Select the **Save as monitoring station assignment** checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.
   c. Select the **Save as user assignment** checkbox if you want to log onto the same monitor zone EVERY time you log in. This is a persistent assignment. You will not be prompted to select a monitor zone during future log ins. This checkbox is only enabled if the user has permission. To restore the prompt to select a monitor zone, simply remove the selection from the User's Monitor Zone Assignment using System Administration.
   d. Click [OK].

**Notes:**
Monitor zone user assignments take precedence over monitoring station user assignments.
For more information, refer to the Monitor Zones Folder chapter in the System Administration User Guide.

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:
   a. Select **No**, if you want all the queued events deleted.
   b. Select **Yes**, if you want all queued event for the monitor zone displayed.

---

**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.

**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].

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].

5. If you are prompted to select a monitor zone:
   a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.
   b. Select the **Save as monitoring station assignment** checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.
   c. Select the **Save as user assignment** checkbox if you want to log onto the same monitor zone EVERY time you log in. This is a persistent assignment. You will not be prompted to select a monitor zone during future log ins. This checkbox is only enabled if the user has permission. To restore the prompt to select a monitor zone, simply remove the selection from the User's Monitor Zone Assignment using System Administration.
   d. Click [OK].

**Notes:**

- Monitor zone user assignments take precedence over monitoring station user assignments.
- For more information, refer to the Monitor Zones Folder chapter in the System Administration User Guide.

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:
   a. Select **No**, if you want all the queued events deleted.
   b. Select **Yes**, if you want all queued event for the monitor zone displayed.

### 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>.”

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.

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].

5. If you are prompted to select a monitor zone:

a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.

b. Select the Save as monitoring station assignment checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.

c. Select the Save as user assignment checkbox if you want to log onto the same monitor zone EVERY time you log in. This is a peristent assignment. You will not be prompted to select a monitor zone during future log ins. This checkbox is only enabled if the user has permission. To restore the prompt to select a monitor zone, simply remove the selection from the User's Monitor Zone Assignment using System Administration.

d. Click [OK].

Notes: Monitor zone user assignments take precedence over monitoring station user assignments.

For more information, refer to the Monitor Zones Folder chapter in the System Administration User Guide.

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:

a. Select No, if you want all the queued events deleted.

b. Select Yes, if you want all queued event for the monitor zone displayed.

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.
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.

Switch Log On

Switch Log On is often used when multiple operators use the same Alarm Monitoring station. Instead of logging out of the application operators can use the switch log on feature. This simultaneously logs out the previous operator and logs in the new operator.

1. Select Switch Log On from the File menu.
2. The Log On to Alarm Monitoring window displays.
3. Enter the user name and password.
4. Select the desired directory.
5. Click [OK].
Notes:  When using switch log on, the person who’s logged into Windows can be a different person than the one logged into Alarm Monitoring.

Switch log on cannot be used if the new user has a monitor zone/user assignment different from the current user.

Log Out of the Application

When you log out of the application the entire application closes.

1. Select Log Off from the File menu.
2. The current user is logged off but the application remains open.

Exit the Application

You can close and exit the application using the following methods:

- Select Exit from the File menu.
- Double-click the icon located in the upper left corner of the title bar. When prompted to log off, click [Yes].
- Single click the icon located in the upper left corner of the title bar and select Close. When prompted to log off, click [Yes].
- Click the close button in the window’s upper right corner. When prompted to log off, click [Yes].
The Main Alarm Monitoring window displays automatically when you log into the application. You can open and close additional windows but the Main Alarm Monitoring window remains open until you log out of the entire application.

Note: You can toggle the display mode of the additional windows between standard and floating behavior that allows you to position the additional windows outside the main Alarm Monitoring window. For more information, refer to Toggle Window Display Modes on page 59.
Menus and Toolbars

The menu bar is a horizontal list of options that appears at the top of the main window. Scroll over each option to view a drop-down menu. A toolbar is a strip of buttons positioned by default just below the menu bar. If you place your cursor over a toolbar button, a tool tip identifies the name of the toolbar button.

Operators can customize how the toolbar displays; they can:

- Change the toolbar from anchored to floating
  Toolbars are anchored by default and 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 window. For more information, refer to How to Use the Toolbars on page 46.
- Control if the toolbar is displayed
  By default the toolbar is displayed. Operators can control if the toolbar is displayed by selecting or deselecting Toolbar from the View menu. For more information, refer to How to Use the Toolbars on page 46.

File menu

Print

Prints information displayed in the active (topmost) window. The print toolbar button does not display if the Main Alarm Monitoring window is minimized.

Log On/Log Off

Logs you into or out of the application.

Switch Log On

Displays the login window, allowing a different user to log in without the previous user manually exiting the application. When the new user is successfully logged in, the old user is simultaneously logged out.

Change Password

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

Exit

Ends the session of every person logged on.

Edit menu

The following menu options are active when an alarm window is displayed.

Acknowledge

Acknowledges the currently selected alarm.
Menus and Toolbars

Fast/Group Acknowledge

Allows a user to acknowledge a group of alarms simultaneously.

Delete

Removes the selected alarm from the window.

Delete All

Removes all alarms from the window.

Select All

Selects all alarms in the window.

View menu

Badge Info

Displays the cardholder folder/window which contains nine forms/tabs: Cardholder, Badge, Access Level, Biometrics, Visits, Assets, Directory Accounts, Guard Tours and Reports. When the cardholder folder/window displays, an additional menu option, Cardholder, displays. For more information, refer to Cardholder menu on page 43.

Visits

Displays the Visits folder/window which contains the Status search, Visit, Details, Email and Reports forms/tabs. From the Visits folder/window you can:

- search visit records based on scheduled time in or out and date and time the record was last changed
- display visit records for a selected date range
- add, modify or delete
- print disposable badges
- sign in or out a visit
- send e-mail notifications
- generate reports

Asset Info

Displays the Asset folder/window which contains the Assets, Assets Classes and Assignments forms/tabs.

System Status

Displays the System Status window which lists all access control devices defined in System Administration.
Device Groups

Displays the various device groups for a particular monitoring zone. Bulk operations can be performed on all parts of the device group. Types of device groups include (but are not limited to) Readers, Cameras and Input and Output groups.

Pending Alarms

Displays the Pending Alarms window. To return to the Main Alarm Monitoring window click the View Alarms toolbar button.

Video Verification

Launches the Video Verification window where you can compare live video to a cardholder’s photograph.

Video Monitoring

Launches the Live Video window which is used to run a video tour of the cameras defined in Camera Groups.

SkyPoint Application

Launches the SkyPoint application for viewing video. This option is only available if you have the SkyPoint client application, which is a separate installation and not included with the OnGuard installation.

Map

Displays a map containing the device associated with the selected alarm (if the Main Alarm Monitoring window is active) or the selected device (if the System Status window is active).

If the selected device is represented on more than one map you will be prompted to select the map of choice. A message displays if the selected device is not represented on any map.

To display the View Map menu option, right-click a device in the System Status window or select an alarm in the Main Alarm Monitoring window. To print a map, select Print from the File menu. The map must be the up most window to print.

Default Map

Displays the map that is assigned to that monitoring zone. This menu option is dimmed if no map has been assigned to this zone.

This menu option is displayed through the Map icon drop-down.

Map Selection

Displays a window in which all available maps are listed. This menu option is dimmed if no map has been assigned to this zone.

This menu option is displayed through the Map icon drop-down.
Menus and Toolbars

Scheduler

Displays the Scheduler window which is used to add, modify and delete scheduled actions within the OnGuard system. An action is any task that can be performed by software as a result of an event of schedule, for example; download a database, mask/unmask alarm inputs, pulse open a door and reset the use limit.

The Scheduler window is also available by selecting Administration > Scheduler in System Administration. For more information, refer to the Scheduler Folder chapter in the System Administration User Guide.

Reports

Displays the Reports folder/window of data entry forms-tabs.

Sort by

Sorts alarms according to criteria chosen in the submenu.

Toolbar

Displays the toolbar when selected (checked).

Status Bar

Displays the status bar when selected (checked).

Trace menu

Monitor Zone

Monitors or traces alarms for the selected monitor zone.

Area

Monitors or traces alarms for the selected intrusion area.

The Area menu option becomes active (not grayed out) when you highlight a device in the System Status window.

Asset

Monitors or traces alarms for the selected asset.

The Asset menu option becomes active (not grayed out) when you highlight a device in the System Status window.

Badge

Monitors or traces alarms for a specific badge.

Controller

Monitors or traces alarms for the selected access panel/controller. An access panel/controller is a device that acts as the focal point for a group of card readers.
The **Controller** menu option or toolbar button becomes active (not grayed out) when you highlight an access panel/controller or any device under a given access panel/controller in the System Status window.

Access panel/controller traces are recursive, meaning all events occurring on that access panel/controller are included.

**Device**

- Monitors or traces alarms for the selected device. The **Device** menu option becomes active (not grayed out) when you highlight a device in the System Status window. This menu option is displayed through the Trace icon drop-down. This menu option can be used to trace all device types including alarm outputs, reader aux inputs and reader aux outputs.

**Configure menu**

**Alarm Filter**

- Displays a checklist of alarm types to monitor. The **Alarm Filter** menu option becomes active (not grayed out) when you display an alarm window.

**Columns**

- Displays a list of columns from which to display. The **Columns** menu option becomes active (not grayed out) when you display an alarm window.

**Hardware Status Frequency**

- Determines how often background updates are performed. The choices are “No Updates”, 10, 15, 20, 30 and 60 minute intervals.

**System Status Options**

- Displays the System Status Options window which is used to specify how the System Status window displays information and what devices are included.

**Control menu**

**Update All Hardware Status**

- Updates the status of all controllers in the monitoring zone.

**Set All Controller Clocks**

- Sets the clocks in all access panels according to the machine on which the driver is running.

**“Current Device”**

- This menu option is dynamic, meaning the name of this menu option changes according to the device highlighted in the System Status window.

  - For example if an LNL-1300 HID reader is highlighted in the System Status window, then LNL-1300 HID displays in the Control menu options.

  - Each “Current Device” menu option also has sub-menu options. For more information refer to Control menu - “Current Device” sub-menu on page 37.

**Guard Tour**

- Allows Operators to launch or view a guard tour. 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.
Menus and Toolbars

To use guard tour the Linkage Server must be properly configured. For more information, refer to the System Options Folder chapter in the System Administration or ID CredentialCenter User Guide.

Control menu - “Current Device” sub-menu

The “Current Device” sub-menu options that are available depend on the type of device listed as the “Current Device” in the Control menu. The type of device listed as the “Current Device” in the Control menu depends on the device highlighted in the System Status window.

**Current Status**
Displays current status of device.

**Acknowledge**
Acknowledges the selected alarm.

**Trace**
Traces the selected device.

**Update Hardware Status**
Polls currently selected access panel/controller and updates the hardware status. If a downstream device (like a reader) is selected, the update hardware status is done for the controller associated with that device.

**Properties**
Displays access panel/controller properties.

**Open Door(s)**

Pulses open any door associated with selected access panel/controller or reader. To activate the Open Door(s) toolbar button you must select an access panel/controller or reader, otherwise the option is grayed out.

**Set Controller Clock**
Sets selected access panel/controller clock to current time. If a device other than an access panel/controller is selected, this option sets the clock on the access panel/controller to which the device is attached.

**Reader Access Modes**
Updates the reader mode of every reader associated with selected access panel/controller or reader.

**Reader Biometric Verify Mode**
Enables/disables verify mode for access control readers with an associated biometric reader. When verify mode is enabled, the normal card and/or pin access is and a biometric match is required. When verify mode is disabled, only the card and/or pin access is required.

**Reader First Card Unlock Mode**
Enables/disables the Reader First Card Unlock Mode. The Reader First Card Unlock Mode is a qualifier for online Reader Mode. When enabled, the online Reader Mode is in effect until the first
(qualified) access granted with entry occurs. When the first access granted with entry occurs, the online Reader Mode changes to unlocked.

Whenever a Reader enters or leaves First Card Unlock Mode, an event transaction is logged in the database and displayed in Alarm Monitoring.

The Reader First Card Unlock Mode can also be enabled/disabled via the Reader folder/window in System Administration, via local timezone control in the LNL-2000 and as part of the Reader Mode or Reader Group Mode action used in the Scheduler and Global I/O.

Reader First Card Unlock Mode is only supported on the LNL-2000 controller. However, first style unlock behavior can be configured for use with any access controller through Lenel’s Global I/O Support.

**Activate**
Activates the selected alarm output.

**Deactivate**
Deactivates the selected alarm output.

**Pulse**
Pulses an output device.

**Mask**
Masks an input device. The System Status window displays masked beside the selected device.

**UnMask**
Unmasks an input device.

**Receiver account information**
A receiver is a piece of hardware used to receive events from multiple accounts in multiple formats. Downstream devices connect to receivers via phone lines, direct wire connections and LAN connections. The receiver account information displays information about a specific receiver.

**View Map**
Displays a map associated with the selected device (if one exists). If more than one map exists, the user is prompted to select a map.

**Launch Video**
Displays video for the selected device if a camera is associated with the device.

**Download Firmware**
Downloads firmware to the following downstream devices: Dual Interface Rdr1 readers, LNL-1100 and LNL-1200 alarm panels, and RS-485 command keypads. It is not possible to download firmware to a single reader interface.

**Download Database**
Downloads the database to the access panel/controller.

**Reset Use Limit**
Resets the number of times a badge can be used on a particular access panel/controller.

**Connect**
Connects the access panel/controller via a dialup/modem connection.
Menus and Toolbars

Disconnect
Disconnects the access panel/controller via a dialup/modem connection.

Execute Custom Function
Executes a custom function associated with the Bosch Intrusion Controller. This menu option is only available with Bosch Intrusion Controllers.

Bypass
Term used to indicate that the zone has been masked. If a zone is bypassed the controller ignores any tamper or alarm condition for the zone.

Unbypass
Similar to bypass, this command unmask the zone so that any tamper or alarm will be reported.

Options menu

Mute Sound
Disables the audio portion of the system when selected (checked).

Font
Selects the font used in Alarm Monitoring.

Save Alarms on Exit
Saves all currently displayed alarms at the end of a session, when selected (checked).

Save Settings on Exit
Saves screen characteristics at the end of a session, when selected (checked). The following settings will be saved for the current user’s profile:

- Window positions, sizes, and minimized states
- Matrix or player mode
- Window arrangement setting
- Scale factor
- List of live and recorded video windows
Windows playing video from a file will not be saved. When the user logs back in, all the video windows previously saved will automatically be launched. Recorded video windows will be launched as live video, since recorded video time is typically not relevant later.

Save Settings Now
Saves screen characteristics immediately.

Ascending Time/Date
Lists alarms in ascending order of time and date (i.e., oldest first), when selected (checked).

Descending Time/Date
Lists alarms in descending order of time and date (i.e., newest first), when selected (checked).

Display Seconds
Includes seconds in the displayed alarm times, when selected (checked).
Auto Cardholder Display for Access Alarms
Displays the cardholder associated with an incoming alarm whenever the alarm deals with a badge id.
If selected (checked), Alarm Monitoring displays the cardholder associated with access alarms.
If not selected (unchecked), Alarm Monitoring does NOT display the cardholder associated with access alarms.

Automatic Map Display
Automatically displays a map when the alarm arrives, if selected (checked) and if the associated device exists on a map. If the device exists on multiple maps, the first one found will be displayed.
This feature must also be configured in System Administration Monitoring > Alarm Configuration menu, Alarm Definitions tab/form.

Automatic Cardholder Display
Applies to alarms for which the Show Card Holder check box is selected in the System Administration software. To locate this check box select the Monitoring menu and then select Alarms. Click the Alarm Definition tab.
If selected (checked), the corresponding cardholder view automatically displays when the alarm arrives if the alarm is related to a badge id.
If the cardholder view is already displayed when a new alarm arrives, the new cardholder associated with the alarm is searched for and displayed.
If not selected (unchecked), the corresponding cardholder view does not automatically display when an alarm occurs.

Automatic Video Verification
Applies to alarms for which the Video Verification check box is selected in the System Administration software. To locate this check box select the Monitoring menu and then select Alarms. Click the Alarm Definition tab.
If selected (checked), the corresponding video verify view automatically displays when the alarm occurs.
If not selected (unchecked), the corresponding video verify view does not automatically display when the alarm occurs.

Automatic Visual Notification
Causes breakthrough alarms to occur. By default, this menu choice is selected (checked) in Alarm Monitoring.
If selected (checked), breakthrough alarms cause the Monitoring application and the Main Alarm View to be brought to the foreground when an alarm occurs.
If not selected (unchecked), breakthrough alarms occur in the background.
Automatic visual notification must be configured for individual alarms in System Administration. From the Monitoring menu select Alarm Configuration. Click the Alarm Definition tab. Highlight the appropriate alarm, click the [Modify] button, select the Visual Notification check box. Click the [OK] button. In the Alarm Monitoring application be sure to refresh the Alarm configuration through the Options menu.

Automatic Live Video Display
Displays live video automatically when an alarm occurs, if selected (checked).
Launch Video for Active Alarm
Displays the video for the active alarm. When the video is launched from a restored alarm the start time of the video clip will be the actual alarm time minus the pre-roll time.

PTZ Options
Displays the PTZ Options dialog which is used to specify locking options, the default PTZ mode, and step mode options.

SkyPoint Options
Displays the SkyPoint Options dialog which is used to specify full screen or windowed display, window resolution, and monitor that will be used for the application.
This dialog is only available if you have the SkyPoint application installed.

Display Status On Maps
Displays the status of all device icons on graphical maps.
If selected (checked), the status of every device icon on a graphical map is displayed (e.g. reader mode, online/offline, occupancy number).
If not selected (unchecked), the status will only be displayed for a given device as a tool tip when the mouse pointer is over the device icon.

Highlight Entire Row
Highlights the entire row of an alarm when selected (checked).

Disable Command Verification
Displays “successful configuration” messages when commands to hardware, E-mail and pages are successfully sent.
If selected (checked), Alarm Monitoring will NOT display “successful configuration” messages.
If not selected (unchecked), Alarm Monitoring displays “successful configuration” messages.
Errors display in message boxes regardless of this setting.

Execute Command on Single Click of Icon
Specifies commands to be executed on a single click. This setting may be configured for each user and saved along with other user settings.
If selected (checked), then a single click executes the default command for the device configured in System Administration.
If not selected (unchecked), then the default command executes on a double-click.

Display Controller Capacity
Displays available memory, free memory, the maximum number of cardholders, current cardholders stored in a controller, maximum number of biometric templates and the current number of biometric templates set in a controller. This information is displayed in the System Status window and is mainly used for diagnostic purposes. By default, this option is unchecked.
If selected (checked), the controller capacity information displays.
If not selected (unchecked), the controller capacity information is NOT displayed.

Display Device Firmware Versions
Displays firmware version (major and minor) for downstream devices. The minor firmware version number displays as the last two digits. The firmware version of controllers and gateways displayed regardless of this option.
The firmware version is that of the interface board.
If selected (checked), the current firmware version displays for devices including single interface readers, dual interface Rdr1 readers, LNL-1100 and LNL-1200 alarm panels, cameras and RS-485 command keypads.
If not selected (unchecked), the firmware version displays as part of the status when the mouse pointer is over the device icon. However the firmware version of controllers and gateways always displays, regardless of this option.

**Display Device Serial Numbers**
Displays the serial number of most devices. The serial numbers are displayed in the System Status Tree for all devices that report a serial number.
Lenel Dual Interface Rdr 2 readers and biometric readers do not report serial numbers. and biometric readers do not report serial numbers.
If selected (checked), the serial number information displays.
If not selected (unchecked), the serial number information is NOT displayed.

**Refresh Alarm Configuration**
Causes alarm configuration information to be refreshed.

**Window menu**

**Cascade**
Places all open windows in an overlapping arrangement with the active window displayed on top.

**Tile Horizontally**
Places all open windows in a horizontal, non-overlapping arrangement.

**Tile Vertically**
Places all open windows in a vertical, non-overlapping arrangement.

**Arrange Icons**
Places all minimized windows (title icons) in a row.

**Close “options”**
There are several menu options to close different windows in the Alarm Monitoring application (e.g. Close All Windows, Close System Status Windows).

**Numbered choices**
Lists all open windows. The active (topmost) window is indicated by a checkmark.

**Help menu**

**Contents**
Displays online help for the currently displayed window.

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

Index
Displays the online help table of contents.

About Alarm Monitoring
Displays version and copyright information.

Cardholder menu
This menu is only available after you select View > Badge Info from the menu options.

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 Anti Pass Back (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
The Bulk sub-menu is only available when the Cardholder menu is available. The Bulk sub-menu options are available when a cardholder record is displayed in the Cardholders folder/window.

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/window: 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.

When bulk changing the Use Limit field and enter no value it will automatically be set to 255 (unlimited).

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**
Displays the Log Viewer window from where you can view a log of bulk events.

**Asset menu**
This menu is only available after you select View > Asset Info from the menu options.

**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 folder/window.

**Asset Types and Subtypes**
Displays the Asset Types and Subtypes Management folder/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**
Enables you to quickly enter multiple Scan IDs for the same type of asset (e.g. enter multiple Scan ID’s for 10 portable PCs). To display the **Bulk Add Mode** menu option an asset record must be open in the Assets folder/window.
How to Use the Toolbars

Alarm Monitoring utilizes one standard Windows toolbar.

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Procedure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the name of a toolbar button</td>
<td>Point to the toolbar button with the mouse (without clicking).</td>
</tr>
<tr>
<td>Use a toolbar button to perform a command or function</td>
<td>Click the toolbar button with the left mouse button.</td>
</tr>
<tr>
<td>Change the toolbar from “anchored” to “floating”</td>
<td>Double-click an empty area of the toolbar.</td>
</tr>
<tr>
<td>Change the toolbar from “floating” to “anchored”</td>
<td></td>
</tr>
<tr>
<td>Hide or display the toolbar</td>
<td>From the View menu select Toolbar. A checkmark appears next to the toolbar if it is not hidden. Toggle the toolbar to display or hide.</td>
</tr>
</tbody>
</table>

Alarm Monitoring Status Bar

The Alarm Monitoring status bar, located in the lower portion of the screen provides different information, depending on what window is displayed.

The Main Alarm Monitoring window displays the following information in the status bar:

- Selected alarm: the name of the selected alarm, if any. If multiple alarms are selected simultaneously, the last one that was selected is indicated here.
- Sort criteria: the information by which the list of alarms is currently sorted.
- Pending: the number of alarms that are currently pending. Pending alarms include all existing normal or initiating alarms marked as “Active” that are still displayed in the main alarm view and have not been acknowledged.
- Total: the total number of alarms currently in the window.
- Verified mode enabled: an access control reader that has an associated biometric reader, is in verify mode.
System Administrator Procedures
The Alarm Monitoring application is not only designed to monitor alarms and events, but it can also be used for a variety of administrative tasks such as adding cardholders or visitors, printing badges, adding assets to the database and assigning assets to cardholders. Depending on how the System Administrator sets the cardholder and system permissions, users with access to Alarm Monitoring can add, modify and delete cardholder, badge and asset information as well as capture images and perform bulk operations.

This chapter assumes that an Alarm Monitoring Station has been physically set up and focuses on the procedures the System Administrator should complete to enable procedures to be performed by Alarm Monitoring Operators. Refer to the OnGuard release notes to determine the PC requirements for an Alarm Monitoring Station (client or server) and refer to the Digital Video Hardware Installation Manual for physically setting up the hardware.

**Administrative Procedures Checklist**

The administrative procedures are completed via the *Administration* menu in the System Administration application. Instructions can be found in the Administration section of the System Administrator User Guide.

- Create card formats - card formats (asset, magnetic, smart card, etc.) are required to configure a reader
- Create badge types - (employee, visitor, etc.)
  - printing/encoding badge options
  - required cardholder fields
  - badge ID allocation for generating ID numbers
  - guest defaults (extended strike/held times, passage mode, deadbolt override)
- Add directories - required for single sign-on
- Set system, cardholder, monitor and field/page permissions
- Add users
  - user name
  - internal account and password
- directory account
- segment access
- area access manager levels

- Add Alarm Monitoring workstations - workstations are required to configure hardware devices
  - add dot matrix printer via workstations folder
  - connect a printer locally (directly to the Alarm Monitoring workstation).

- Set general system options
  - log on authorization warning
  - strong password enforcement
  - number of days to save queued events
  - Linkage Server host
  -DataExchange server host

- Set cardholder options and visits
  - maximum number of badges per cardholder
  - ability to create/save photo thumbnails
  - badge PIN types (4, 6 or 9-digits)
  - PIN code generated (random or manual)
  - precision access mode
  - use or lose badge feature (change badge status to lost or returned after a specified amount of time)
  - visits options
  - cardholder, visitor and visit search result options

- Configure global output devices
  - SMTP server settings to use when sending e-mail
  - GOS paging device
  - recipients of e-mail and page messages

- Configure e-mail and paging notification
  - fields and display order for e-mails and paging
  - fields and/or directories to check when determining who to send an e-mail notification to

- Add segments to your installation
  - enable segmentation
  - segment options

- Create list options (using List Builder)

- Set up archiving parameters

Access Control Procedures Checklist

This portion of the chapter focuses on the procedures the System Administrator should complete to enable access control and monitoring procedures to be performed by Alarm Monitoring Operators.

Note: Be sure to complete the administrative procedures listed at the beginning of this chapter before attempting any access control and monitoring procedures. Several access control and monitoring procedures require that certain administrative procedures be completed.
first. For example you must configure a workstation before you can configure most hardware devices.

All System Administrator access control procedures are completed via the Access Control or Additional Hardware menu in the System Administration application. Instructions can be found in the Access Control section of the System Administration User Guide, as well as the Additional Hardware section. A separate Intrusion Detection User Guide also exists if you are going to configure intrusion detection devices.

- Configure hardware devices
  - dialup modem
  - access panels
  - readers
  - alarm panels
- Additional access control configurations
  - timezones (specify holidays, assign readers and modes of operation)
  - access levels
  - anti-passback areas (normal, safe and hazardous areas for mustering)
  - alarm mask groups (un/mask multiple alarm inputs simultaneously)
  - device groups (input/output readers)
  - local and/or global inputs and outputs
- Configure additional hardware
  - fire panels
  - intercom devices
  - personal safety devices
  - receivers
  - intrusion detection devices

**Intrusion Detection Alarm Definitions**

See the Alarm Definitions appendix in the Intrusion Detection User Guide for information on alarm definitions in references to customizing intrusion detection alarms.

**Alarm Monitoring Operator Procedures**

These procedures are used to handle intrusion detection events in Alarm Monitoring. For specifics see the Alarm Monitoring Operator Procedures chapter in the Intrusion Detection User Guide.

**Intrusion Detection Device Statuses**

See the Intrusion Detection Device Statuses appendix in the Intrusion Detection User Guide for more information.
Monitoring Procedures Checklist

System Administrator monitoring procedures are completed via the Monitoring menu in the System Administration application. Instructions can be found in the Monitoring section of the System Administration User Guide.

- Customize alarms, instructions, acknowledgment notes and acknowledgment actions
  - alarm mask groups
  - customize and configure alarms
  - text instructions
  - audio
  - acknowledgment notes
  - automatic acknowledgment actions
- Configure monitor zones
  - event routing group
  - monitor zones
  - monitoring station assignments
- Set up guard tours
  - checkpoint actions
  - messages and checkpoint events
  - monitoring stations
  - link camera devices to the checkpoints
  - special instructions
- Set Monitoring Options
  - associate a command with a device or area icon (enables operators to execute a command with a single and double left-click in the system status tree and map view)

Video Procedures Checklist

All the video procedures are completed via the Video menu in the System Administration application. Instructions can be found in the Video section of the System Administration User Guide.

- Configure video
  - matrix switcher
  - video devices (recorders and cameras)
  - link hardware devices to a camera
  - alarm-video configurations
  - add a video recorder to a monitoring zone
- Configure video verification
  - CCTV Controller associated with a workstation

CCTV Command (located on Access Control > Readers > Control tab)
Operator Procedures
Several windows in Alarm Monitoring can be configured to display according to user preference. These views are recreated every time the user logs into the application.

The following is a list of user-defined display options that are set from the Configure or Options menu.

- Select Event Types to Monitor on page 57
- Select Column Configuration on page 58
- Set Automatic Display Options on page 59
- Select Hardware View Options on page 61

**Note:** The Select Hardware View procedure displays the System Status Options Window.

- Toggle Window Display Modes on page 59
- Display Multiple Windows in the Main Window on page 60

**System Status Options Window**

The System Status Options window is displayed from the System Status window. Verify you are in the System Status window, then select Configure > System Status Options from the menu.

You can also display the System Status Options window by clicking the System Status icon that displays to the left of the File menu (when you open the System Status window).
All devices
Displays all the devices (active, offline, runaway, masked, armed, disarmed, and areas in alarm) in the System Status window.

Specified devices
Displays specific types of devices.

Active devices
Displays only active devices in the System Status window.

Offline devices
Displays only offline devices in the System Status window.

Runaway devices
Displays only runaway devices in the System Status window.

Masked devices
Displays only masked devices in the System Status window.

Armed areas
Displays only armed areas in the System Status window. An area is a separately configured section of an Intrusion Detection Panel, sometimes referred to as a partition. To arm an area means to “turn on” the protection for an area.

Disarmed areas
Displays only disarmed areas in the System Status window.

Areas in alarm
Displays only areas that have an active alarm triggered. If one or more of the specified device selections are made, only devices matching those criteria display in the view.

View
Displays information about devices in one of three (3) modes.
Display Option Procedures

Use the following procedures to customize the display.

Select Event Types to Monitor

If you have permission to edit alarm filters, you can apply an alarm filter to each view in Alarm Monitoring, including the main alarm view, pending alarm view, video verification view and any trace view. Each of these views can be configured to filter out alarms independent of each other, however, only the main alarm view filter is saved from session to session. The alarm filter determines which alarms display based on the type of event the alarm is associated with.
For example, you may wish to display every alarm for a specific reader’s trace window but you may not wish to display “Access Granted” alarms in the Main Alarm Monitoring window. You can apply both of these filters to the different views, but when the session ends, only the filters applied the main window are saved.

1. Open the window from which you want to select the events displayed. Verify this window is the active (topmost) window.

2. From the Configure menu, select Alarm Filter. The Alarm Filter window displays.

3. By default, all event types are selected (have a check mark). If you do not want to display a particular category of events, click that option to deselect it (remove the check mark). Click the option again to select it.

4. Click [OK] to close the Alarm Filter window

### Select Column Configuration

You can rearrange the order of the columns in any window as well as add or remove columns that display. This is done independently for each type of window. For example, if the column configuration is changed for an alarm window, this becomes the default for all alarm windows of the same type. If the column configuration is changed for a given reader trace, this will become the default configuration for all reader traces.

1. Open the window from which you want to configure the columns displayed. Verify this window is the active (topmost) window.

2. From the Configure menu select Columns. The Column Configuration window displays.
3. In the **Select columns** display field, click/highlight the name of a column, then click [>>]. The column name appears in the **Columns to view** display field.

4. Arrange the column names in the order you want them to appear. Click/highlight a column name in the **Columns to view** display box. Then use the [Up] and [Down] buttons to change the column’s relative position.

**Note:** The order the column names appear in the **Columns to view** display field is the same order the columns will display in the window which you are configuring the columns for.

5. Click [OK] and the window displays the new column configuration.

### Set Automatic Display Options

Several display options are available from the **Options** menu. To activate an option select it (place a check mark beside it). To deactivate an option select it again to remove the check mark. For information on the options available from the **Options** menu, refer to Chapter 2: Main Alarm Monitoring Window on page 31.

### Toggle Window Display Modes

In Alarm Monitoring, you can use the following options from a window’s shortcut menu to switch between the window display modes. (Open the shortcut menu by left-clicking on the icon in the window’s title bar.)
- Standard Mode - This is the default window display mode. When this mode is selected, the window cannot be moved outside of the main Alarm Monitoring window. For more information, refer to Display Multiple Windows in the Main Window on page 60.
- Floating Mode - When this mode is selected, the window is independent of the main Alarm Monitoring window, and can be moved (dragged) outside the main window onto one or more monitors:

Floating windows contain the main window menu bar and appear in the Windows taskbar. In addition, the *Always on top* menu option is available for floating windows. When *Always on top* is selected, the window remains in view when you switch to a different window.

The following windows can display in the floating mode:
- Main Alarm Monitor
- Pending Alarms
- Trace Monitors
- System Status
- Map views
- Cardholder Verification
- Video Verification
- Video Monitoring

**Display Multiple Windows in the Main Window**

For windows in the standard display mode, complete the following steps:
1. Open the desired windows using the toolbar buttons or menu options.
2. From the *Window* menu, select one of the following:
   - Cascade
   - Tile Horizontally
Display Option Procedures

- Tile Vertically

3. Using the mouse, click and drag each window to resize and relocate it.

Select Hardware View Options

Hardware view options include list or tree view as well as the type of devices displayed. Users can display every device or select devices that meet a specific criteria such as active, offline, runaway, and/or masked devices as well as armed areas, disarmed areas and/or areas in alarm.

1. Verify you are in the System Status window, then select Configure > System Status Options from the menu.

2. The System Status Options window displays.
   a. Select the type of device you would like to display by clicking either the All devices or Specified devices check box. If you selected the Specified devices check box, select the desired device by clicking the appropriate radio button (active, offline or masked devices).
   b. Select the Tree radio button to view the system hardware in a tree or branching format.
   c. Select the Tree (area-based) radio button to view NGP devices in an area-based branching format.
   d. Select the List radio button to view a list of devices, their current status and parent device.
   e. Select the Lock display updates check box if desired.

3. Click [OK].
The System Status window and Device Groups window are used to monitor devices.

**System Status Window**

The System Status window lists every access control device, area or action group defined in System Administration for a specific segment. Other configuration settings are listed in parenthesis after each device.

The System Status window can be displayed several ways:

- Click the triangle on the System Status button and select an existing window or open a new one.

**Note:** Clicking the System Status button (not the triangle) brings up a new System Status window if there is none present. If a System Status window is already open, clicking the System Status button causes the default (first) window to display.

- From the *View* menu, select *System Status* and then the window you want to display.
- Click the System Status toolbar button.

- Choose one of the numbered options under the *Window* menu.
  - Though rare, if more than nine (9) System Status windows are open, the *More Windows* menu option will be available. Choose a window from the list and click [OK] to bring it to the foreground.
Display window
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. 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. An icon to the left of each entry identifies the entry’s type.

Hardware Status Bar
Located on the lower right portion of the screen, the status bar on the System Status window has four counters:

- Viewing: Shows the number of devices viewed.
- Active count: Shows the number of active points in the monitoring zone. This is NOT the same as the number of active devices. For example, if a reader is in the Door Forced Open, Door Held Open and Reader Tamper states, the active count is increased by three. The active device number is not increased.
- Offline count: Shows the number of offline devices in the Monitoring Zone. Every device is counted including alarm inputs, reader auxiliary inputs, alarm outputs and reader auxiliary outputs.
- Mask count: Shows the number of masked points in the monitoring zone.

MUSTER MODE: This portion of the status bar only displays when a Monitoring Zone is in Muster mode.

Device Groups Window
The Device Groups window displays the currently configured device groups within a monitoring zone and is expandable in the tree view. The Device Groups window allows operators to view, test and change the status of devices (cameras, remote monitors, readers, inputs and outputs).

Toolbar Shortcut
Device Group Test Mode Window

To display the Device Groups Window, click the View Device Groups toolbar button or select **Device Groups** from the **View** menu.

### Device Group Test Mode Window

Similar windows display for the test access grants, test forced open and test inputs for device groups. The example below is a Test Inputs for an input device group.

![Test Inputs for Main Building: Input Device Group](image)

<table>
<thead>
<tr>
<th>Alarm Description</th>
<th>Time/Date</th>
<th>Controller</th>
<th>Device</th>
<th>Input/Output</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Active</td>
<td>3:20 PM</td>
<td>LVR-162</td>
<td>Axis 201 Input 2</td>
<td>2</td>
<td>200</td>
</tr>
</tbody>
</table>

**Upper status bar**

Displays information about the upper display window and includes the total number of devices tested, the number of devices that pass and fail, what time the test started and the current status of the device test.

**Upper display window**

Displays the device name, test status, alarm description, number of inputs or requests received and the current device status. The information displayed in this window can be sorted by any column.

**Lower display window**

Displays a variety of user-defined columns that can be sorted. Users can select whether the following columns display: Alarm Description, Time/Date, Controller, Device, Input/Output, Card, Priority, Asset Scan ID, Asset Name, Intercom Station Called, Controller Time, Transmitter, Transmitter Input, Biometric Score, Account Group, Badge Type, Text, Line Number and Intrusion Area. For more information, refer to **Select Column Configuration** on page 58.

**Lower status bar**

Displays information about the lower display window and includes the name of the currently selected alarm, sort criteria, trace type and the total number of alarms listed.
Device Group Icons

The table below identifies the different icon groups available.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>OnGuard System</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Alarm Mask Group</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Camera Group</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Reader Group</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Alarm Input Group</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Alarm Output Group</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Monitor Group</td>
</tr>
</tbody>
</table>

Hardware Device Icons

The table below identifies the different icons available. To view a list of icons and icon groups available in your database, as well as add or modify icons, open MapDesigner and select Edit > Icon Library.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Access Panel</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Access Panel with selective cardholder download enabled.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Alarm/Camera/Reader Input</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Alarm/Camera/Reader Output</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Alarm Panel</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Camera</td>
</tr>
<tr>
<td>![Icon]</td>
<td>The Camera icon flashes when there is motion detected with the associated camera. The CCTV Camera icon turns green when there is sound with the associated camera.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>CCTV Monitor</td>
</tr>
<tr>
<td>![Icon]</td>
<td>CCTV Panel</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><img src="image" alt="Facility Utilization Gate" /></td>
<td>Facility Utilization Gate</td>
</tr>
<tr>
<td><img src="image" alt="Fire Panel" /></td>
<td>Fire Panel</td>
</tr>
<tr>
<td><img src="image" alt="Function List" /></td>
<td>Function List</td>
</tr>
<tr>
<td><img src="image" alt="IntelligentVideo Application" /></td>
<td>IntelligentVideo Application</td>
</tr>
<tr>
<td><img src="image" alt="IntelligentVideo Server" /></td>
<td>IntelligentVideo Server</td>
</tr>
<tr>
<td><img src="image" alt="Intercom Exchange" /></td>
<td>Intercom Exchange</td>
</tr>
<tr>
<td><img src="image" alt="Intercom Station" /></td>
<td>Intercom Station</td>
</tr>
<tr>
<td><img src="image" alt="Intercom Station Analytics Event" /></td>
<td>Intercom Station Analytics Event</td>
</tr>
<tr>
<td><img src="image" alt="Intercom Station Call Connected" /></td>
<td>Intercom Station Call Connected</td>
</tr>
<tr>
<td><img src="image" alt="Intercom Station Line Error" /></td>
<td>Intercom Station Line Error</td>
</tr>
<tr>
<td><img src="image" alt="Intercom Station Queued" /></td>
<td>Intercom Station Queued</td>
</tr>
<tr>
<td><img src="image" alt="Intrusion Area" /></td>
<td>Intrusion Area</td>
</tr>
<tr>
<td><img src="image" alt="Intrusion Door" /></td>
<td>Intrusion Door</td>
</tr>
<tr>
<td><img src="image" alt="Intrusion Offboard Relays" /></td>
<td>Intrusion Offboard Relays</td>
</tr>
<tr>
<td><img src="image" alt="Intrusion Onboard Relays" /></td>
<td>Intrusion Onboard Relays</td>
</tr>
<tr>
<td><img src="image" alt="Intrusion Panels" /></td>
<td>Intrusion Panels</td>
</tr>
<tr>
<td><img src="image" alt="Intrusion Zones" /></td>
<td>Intrusion Zones</td>
</tr>
<tr>
<td><img src="image" alt="Matrix Switcher" /></td>
<td>Matrix Switcher</td>
</tr>
<tr>
<td><img src="image" alt="DataConduIT Device" /></td>
<td>DataConduIT Device</td>
</tr>
<tr>
<td><img src="image" alt="DataConduIT Source" /></td>
<td>DataConduIT Source</td>
</tr>
<tr>
<td><img src="image" alt="DataConduIT Sub-Device" /></td>
<td>DataConduIT Sub-Device</td>
</tr>
<tr>
<td><img src="image" alt="PC Panel" /></td>
<td>PC Panel</td>
</tr>
<tr>
<td><img src="image" alt="Personal Safety Device Panel" /></td>
<td>Personal Safety Device Panel</td>
</tr>
</tbody>
</table>
Alarm Monitoring User Guide

Monitor Devices

Device Status

Alarm Monitoring is the only application that displays the status of hardware devices. Alarm Monitoring obtains the status of a device from the Communication Server, which in turn obtains the device status from hardware controllers.

Status icons are located to the left of hardware device icon. There may be one icon or a combination of icons, depending on the hardware status.

The status of the device is displayed after the entry in parentheses. If viewing the icons on a map, the device status is displayed in parentheses after the icon or as a tool tip when the mouse pointer is over the device icon. This is determined by whether the Display Status on Maps option in the Options menu is checked.

Note: To view a list of current hardware status icons in your database, as well as add additional icons, open MapDesigner and select Edit > Icon Library.

Runaway Devices

When configured conditions cause a device to enter a “runaway” state, an alarm is generated and the status information displayed next to the device icon is updated to indicate it is a runaway device. A runaway device is characterized by multiple alarms of the same type coming from the device during a user-defined time interval. While the device is in the runaway 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 occurs and the status information for the device is updated to normal in the hardware tree.

Runaway device conditions are configured on the System Options > Runaway Detection tab in System Administration.

Offline Hardware Devices

**IMPORTANT:** The Communication Server must be running in order for the proper offline status to be reported in Alarm Monitoring.

Devices can be marked offline for two reasons: The connection may be broken or it can intentionally be set offline. In Alarm Monitoring a different color “X” is used to differentiate those items that are intentionally taken offline to those that have a broken connection.

---

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="reader_icon.png" alt="Reader Icon" /></td>
<td>Reader</td>
</tr>
<tr>
<td><img src="receiver_icon.png" alt="Receiver Icon" /></td>
<td>Receiver</td>
</tr>
<tr>
<td><img src="remote_monitor_icon.png" alt="Remote Monitor Icon" /></td>
<td>Remote Monitor</td>
</tr>
<tr>
<td><img src="video_cell_icon.png" alt="Remote Monitor Video Cell Icon" /></td>
<td>Remote Monitor Video Cell</td>
</tr>
<tr>
<td><img src="segment_icon.png" alt="Segment Icon" /></td>
<td>Segment (only if your system is segmented)</td>
</tr>
</tbody>
</table>
Device Status

Broken Connection
A red “X” through an icon indicates a broken connection, meaning that the software cannot communicate to the device. For example:

![Bldg. 7 West Door Reader]  
If a child device is offline then the parent device is examined. If both child and parent are found to be offline then a red “X” is used for both devices. If only the child device is offline then a yellow “X” is used for just the child device.

Although surveillance-only cameras are not associated with a physical video recorder, they are assigned to a virtual “surveillance-only recorder” to maintain consistency in the user interface. For example, the Alarm Monitoring hardware tree below shows two surveillance-only cameras assigned to a virtually surveillance-only recorder which serves only as a placeholder to group cameras.

![System Status Tree (all devices)]

A 16-bit OEM code can be programmed into the device which allows for a check to occur in Alarm Monitoring. If the OEM code doesn’t match the hardware, an Invalid ID transaction is generated and the device will not come online. The system status tree will show the status as offline and list the invalid OEM code.

![System Status Tree (all devices)]

Marked Offline
Many items can be marked offline intentionally in System Administration. When items are marked offline, a black “X” appears on those items in Alarm Monitoring. A black “X” also appears for those items that are deleted from the system. Deleted items are also marked with text that reads “deleted.”

A list of items that can be marked offline are: Alarm inputs, Cameras, Camera Inputs, Camera Outputs, Elevator Dispatching Panels, Fire panels, Intercom devices, Intrusion Detection Devices, Lenel access panels, OPC Connections, Personal Safety Devices, POS Devices, Receivers, SNMP Managers, and Video Recorders.

Items that show a black “X” if their parent device has been marked offline include: Alarm inputs, Alarm Mask Groups, Alarm outputs, Alarm panels, Anti-passback areas, Camera Inputs, Camera Outputs, Cameras, Elevator dispatching terminals, Fire Devices, Fire Inputs/Outputs, Intercom stations, Intrusion Areas, Intrusion Doors, Intrusion Onboard/Offboard relays, Intrusion zones, Local function lists, OPC Sources, POS Register, Readers, Reader Inputs, and Reader Outputs.

Map items need to be configured in MapDesigner to use the current state of the device rather than a default icon for the proper icons to be shown on the map.

Video Failover Status
IP camera icons in the System Status Tree display the status of the primary and secondary recorders if failover is enabled. For more information, refer to Video Failover Status Indicators on page 81.
Procedures for Monitoring Devices

Use the following procedures for monitoring devices.

Update the Hardware Status

Hardware status information displays in several Alarm Monitoring windows. When alarms and actions occur in the system, OnGuard software updates the status information “live” for the affected hardware. Operators can also choose to have the status updated on demand.

1. Select **Update All Hardware Status** from the **Control** menu or by right-click an alarm, access panel, alarm panel, alarm input, relay output or reader.
2. The update all hardware status feature polls the currently selected device and updates the hardware status of the associated devices. A message displays when the update is complete.

**Note:** Hardware Status Update Frequency can be used to set automatic updates. You can set the frequency to No Updates, 10, 15, 20, 30 or 60 minutes (by selecting **Hardware Status Frequency** from the **Configure** menu).

Perform a Device Test

Operators can perform a test on various devices in the system. A special test mode operation is available for Input Groups, Reader Groups (Door Forced) and Reader Groups (Access Grants). Performing this test allows you to see which devices generated alarms and which ones did not.

1. Display the Device Groups window by selecting **View > Device Groups**.
2. Right-click the device group and select the **Test Inputs**, **Test Door Forced** or **Test Access Grants**. If you select **Test Access Grants**, skip to step 7.
3. A dialog box appears:

4. You have two choices. Choose **Show alarms only in Test Mode windows** if you do not want the results to show up on any Monitoring Station. Otherwise choose **Show alarms in all windows on all Monitoring Stations**.
5. Type in the duration (in minutes) of the test. This option is available only if you selected **Show alarms only in Test mode windows**.
6. Click [OK] to initiate the test.
7. A Test Mode window launches. The top portion of the window lists all the devices being tested and their current status (whether the test was successful/unsuccessful). Devices that failed the test flash in red. The bottom portion of the window displays a trace of the related alarms.
8. When the test is finished, all the windows and monitoring stations resume their normal display of alarms.

**Note:** Device status is not available for Matrix Switchers or Account Panels.
Procedures for Monitoring Devices

Locate or Search for a Device
Operators can locate or search for a device in any window in Alarm Monitoring.

1. Display any Alarm Monitoring window.
2. Verify your cursor is in the window.
3. Begin typing the name of the device. The system automatically scrolls to the first occurrence of those letters in column one.

View the Last Connection Time for Dialup Panels
The Last connect time status is displayed in parenthesis after each dialup panel. It reflects the time of the panel’s last “Communications Restored” event and is updated every time you disconnect from the panel.

To view a dialup panel’s Last connect time within Alarm Monitoring, locate the dialup panel in the System Status window. In parenthesis after the name of the dialup panel, the Last connect time is listed.

Last Connection Time Guidelines
The following are guidelines for the Last connect time status:

• If a dialup panel has never connected, the Last connect time for it is “Never”.
• If a dialup panel connects while Alarm Monitoring is not running, the Last connect time for it is retrieved from the database when Alarm Monitoring starts up again.
• When a dialup panel is disconnected, the System Status window immediately reflects the new Last connect time regardless of whether the “Communications Lost” alarm is acknowledged or not.
• When a dialup panel and Alarm Monitoring station are in different time zones, the Last connect time displays both the local time and the panel time.

Download the OnGuard Database or Firmware
Operators can download the OnGuard database and/or firmware to devices via Alarm Monitoring. Devices include access panels (LNL-500, LNL-1000, and LNL-2000), dual interface Rdr1 readers, alarm panels, RS-485 command keypads and cameras.

Notes: It is not possible to download firmware to single reader interfaces.
It is only possible to download firmware to LNL-1320 version B dual reader interfaces through the primary reader.
It is only possible to download firmware to LNL-CK command keypads connecting directly via RS-485 interface cable.
It is only possible to download firmware to LNL-500B gateways communicating to Handkey and Bioscrypt Fingerprint Biometric readers (number 0 only).

Toolbar Shortcut

1. Open Alarm Monitoring and display the System Status window by selecting View > System Status and then the desired window.
2. Right-click the device in the hardware view and select Download Database, Download Firmware or Download Reader Firmware.

**View the Controller Properties**

The type of firmware a controller has is indicated in the firmware revision reported in the Alarm Monitoring hardware view. It can also be found in the diagnostic tab of the access panels folder in System Administration and in the main window of the Controller Encryption Configuration Utility, which can be found in the OnGuard directory.

**Note:** If the firmware on the LNL-500, LNL-1000, and LNL-2000 controllers is not up to the latest version that is in the release a “[Not current]” tag will be noted on the firmware version string.

The flash chip size is indicated in the Alarm Monitoring controller properties dialog box, which you get to by right-clicking on the controller and selecting properties. It can also be found in the diagnostic tab of the access panels folder in System Administration.

**Note:** If the current firmware revision in the controller is older then 3.041 the controller will not report its flash size and it will not be indicated in any utility.

The current DIP switch settings for a given controller are indicated in the Alarm Monitoring controller properties dialog box, which you get to by right-clicking on the controller and selecting properties. It can also be found in the Diagnostic tab of the access panels folder in System Administration.

LNL-2000 and LNL-3000 boards show the Communications Path Status, which indicates which of their dual path connections are active. The value of this status can be either Primary or Secondary/Failover. The secondary connection is only used when a problem with the primary problem has occurred. This status can also be seen in the System Status Tree of the controller.

There is an additional property, Selective Cardholder Download, which is either enabled or disabled in the controller properties of an Access Panel. If you update the selective download configuration in System Administration, you can perform an Update Hardware Status in Alarm Monitoring to see the changes.

**View Notes**

Some hardware devices may have notes that were entered in System Administration. This is available for access panels, fire panels, intercom devices, personal safety devices, receivers, intrusion panels, Crestron PLC, POS devices, SNMP managers, readers, elevator dispatching devices, video recorders, and cameras.

To view the device notes:

1. Select the device and right-click on it. Or, if there is an alarm, right-click on the alarm.

2. A popup menu is displayed. If there are no notes, the option will be disabled and labeled with (None). Otherwise, there are a few possible menu options:
   a. Select the View Controller Notes option from the popup menu (for devices that are access panels, fire panels, intercom devices, personal safety devices, receivers, intrusion panels, Crestron PLC, POS devices, SNMP managers, video recorders, or elevator dispatching devices).
   b. If the device you selected is a reader, select View Reader Notes.
   c. If the device you selected is a camera, select View Camera Notes.
d. If you selected an alarm, select **View Device Notes**. If there are associated devices containing notes, they will be shown in a new popup window. Select a device to show the corresponding notes.

3. The Notes window is displayed. These notes are read-only. Click [OK] when you are done to exit.
CHAPTER 6

Trace Alarms and Events

OnGuard allows you to trace the alarms and events associated with a monitor zone, controller, device, badge, asset or area. This includes events from third party DataConduit sources.

**Note:** Trace permissions for a Monitor Permission Group are set in System Administration or ID CredentialCenter in Administration > Users > Monitor Permission Groups tab > Monitor sub-tab.

**Trace Configuration Window Overview**

The Trace Configuration window performs live and historical traces of events and is displayed by:

- Selecting the *Trace* menu and then the type of device you wish to trace. Click [OK] when OnGuard prompts you to verify the name of the device to be traced.
- Right-clicking an alarm and selecting *Trace* and then the device you wish to trace.
- If tracing a badge you are first introduced with the following dialog box. Type the badge ID you wish to trace and click [OK].
Trace Configuration Window

Perform historical trace
If the check box is selected, the trace will include events that occurred between the Start and End date/times you specify.

Today
When clicked, the Start and End fields populate with the following:
- Start and End date: the current day’s date
- Start time: 00:00 on the current date
- End time: 23:59 on the current date

Start
The first date/time combination that the trace displays events for

End
The last date/time combination that the trace displays events for

Apply start and end time to each day
If the check box is selected, the time range is applied to each day within the date range.
For example: A trace has a Start date/time of 12/1/2003 9:00 and an End date/time of 12/9/2003 17:00.
- If the Apply start and end time to each day check box is checked, then the trace will include only those events that occurred during the hours of 9:00 a.m. through 5:00 p.m. on the days December 1st through December 9th, 2003.
- If the Apply start and end time to each day check box is not checked, then the trace will include all events that occurred from 9:00 a.m. on December 1st until 5:00 p.m. on December 9th.

Use restored transactions
This option is applicable only when a historical trace is performed.
- If the check box is selected, restored transactions will be included in the historical trace.
- If the check box is not selected, normal transactions from the EVENTS table will be used for the historical trace.
Procedure for Tracing

Perform live trace
Controls whether new events are displayed or not
– If the check box is selected, the trace displays new events.
– If the check box is not selected, live tracing is disabled and new events are excluded from the trace.

Show only those alarms which have marked video
Controls whether alarms (events) that have marked video are displayed or not.
– If the check box is selected, live tracing shows events that are new AND are configured (in the System Administration application) to have video marked for them. The marking is not instant, so the trace may not show the 🎥 icon in front of the event right away.
– When the Show only those alarms which have marked video check box is checked and the Perform historical trace check box is checked, the trace will show events which have video marked for them, regardless of the current alarm-video configuration in the System Administration application. This means that a video-only trace may exclude some alarms seen in the main alarm view with a 🎥 icon in front of them.

Alarm Filter
Enables you to configure the type of events that will be displayed for a trace. When clicked, the Alarm Filter window opens.

OK
Performs the trace using the settings selected and closes the Trace Configuration window. A Trace Monitor window will open, which looks identical to the Main Alarm Monitoring window, but displays only those alarms that are associated with the trace criteria specified.

Cancel
Cancels the pending requested action.

Help
Displays help for this topic.

Procedure for Tracing

Use the following procedures for tracing.

Trace Alarms and Events
OnGuard allows you to trace the alarms and events associated with a monitor zone, controller, device, badge, asset or area. This includes events from third party DataConduIT sources.

1. Select (highlight) an alarm, event or device you want to trace.
2. Do one of the following:
   • Right-click and select Trace. Then select Controller, Device, Badge, Asset or Area.
   • From the Trace menu select Controller, Device, Badge, Asset or Area.
• Click the toolbar button that corresponds to what you want to trace. Choices include:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Controller Icon]</td>
<td>Traces a Controller</td>
</tr>
<tr>
<td>![Device Icon]</td>
<td>Traces a Device (including alarm outputs, reader aux inputs and reader aux outputs)</td>
</tr>
<tr>
<td>![Badge Icon]</td>
<td>Traces a Badge</td>
</tr>
</tbody>
</table>

Note: If you are tracing a badge the Trace Badge window displays asking you to verify the Badge ID. Click [OK].

3. The Trace Configuration window displays.

4. To perform a historical trace, select the Perform historical trace check box and select the Start and End dates.
   • (Optional) You can also select the Apply start and end time to each day or the Use restored transactions check box.

5. To perform a live trace, select the Perform live trace check box.
   • Show only those alarms which have marked video check box unchecked

6. To view only alarms with video select the Show only those alarms which have marked video check box.

7. Click [Alarm Filter] to select the types of events that will be displayed for this trace.

8. In the Alarm Filter window, select (place a checkmark beside) the alarm types you want displayed.

9. Click [OK].

10. In the Trace Configuration dialog, click [OK].

11. OnGuard will open a new Trace Monitor window that looks identical to the Main Alarm Monitoring window, but only displays alarms that are associated with the trace.
CHAPTER 7

Video Monitoring

The Video Monitoring window displays live video only. To view recorded video you must use the Video Player.

The Video Monitoring window performs the following function:

- Displays live video from one camera at any given time.
- Create a new video tour. For more information, refer to Create a Custom Video Tour on page 80.
- View a video tour. For more information, refer to View a Video Tour on page 81.

The Video Monitoring window is displayed by:

- Selecting the Video Monitoring toolbar button.

  **Toolbar Shortcut**

  ![Video Monitoring Toolbar Icon]

- Selecting View > Video Monitoring from the menu.
Video Monitoring Window

Device Groups listing
Lists the available video device groups. A device group can contain devices from more than one video recorder.

Device groups can also be segmented and belong either to one segment or all segments. If a device group belongs to only one segment, the group will contain only devices associated with the access panel defined for that segment.

Display area
Displays a specific camera view - live.

Video Monitoring Window Procedures

Video Tours
There are two types of tours that can be viewed. A basic Video Tour allows you to select and watch a series of videos in succession. A custom video tour allows you to watch a series of video layouts in succession.

Create a Custom Video Tour
1. In Alarm Monitoring, navigate to View > Video Monitoring.
2. Right-click the Video Tours and select Create New. The Create Video Tour window opens.
3. In the name field, add a friendly name for the video tour.
4. In the Layout column click to add new steps to the video tour. The Load Layout window opens. Select the layout and click [OK].
5. In the Delay column select the delay in seconds for each layout.
6. Click [OK].
View a Video Tour

The Video Tour is used to view a group of cameras successively. These cameras are defined as a device group in the Groups folder of System Administration. The Video Tour feature is only available for online cameras/recorders.

1. Launch the Video Monitoring window by either selecting the Video Monitoring toolbar button or choosing Video Monitoring from the View menu.
2. Verify the cameras/recorders are online. If the device icon does not have a red “X” through it the device is online.
3. Right-click a camera device group and select Video Tour Options. The Video Tour window displays.
4. Select the desired View time and click [OK]. This is the amount of time each camera is displayed in the tour.
5. Right-click the camera device group again and select Start Video Tour. The right side of the window displays the camera views.

View the Custom Video Tour

The Custom Video Tour is used to view a group of camera layouts successively.

1. Launch the Video Monitoring window. In Alarm Monitoring, by either selecting the Video Monitoring toolbar button or choosing Video Monitoring from the View menu. In VideoViewer, select the Tour tab in the Camera Selection window.
2. Verify the cameras/recorders are online. If the device icon does not have a red “X” through it the device is online.
3. Right-click a video tours group and select Video Tour Options. The Video Tour window displays.
4. Select the desired View time. This is the amount of time each camera is displayed in the tour. If in VideoViewer, you can also choose to start the video tour in full screen mode and pause it on exit. Click [OK]
5. Right-click the video tour group and select Start Video Tour. The right side of the window displays the camera views.

Video Failover Status Indicators

IP camera icons in the System Status Tree display the status of the primary and secondary recorders if failover is enabled. The camera icon is divided into two parts, the first half indicates the status of the primary recorder, and the second half of the icon indicates the status of the secondary recorder if redundancy is enabled. If redundancy is not enabled, then there is not a continuous connection to the secondary recorder and the status is not known or displayed in the second half of the camera icon.

The following indicators are used:

- Green box - indicates that the recorder and the camera are online
- Red “X” - indicates that the recorder is offline
- Yellow “X” - indicates that the recorder is online and the camera is offline
• Black “X” - indicates that either the recorder or the camera is logically marked offline in System Administration or through the right-click menu in Alarm Monitoring.

<table>
<thead>
<tr>
<th>Example Icon</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>The primary and secondary recorders are online and both have a valid connection to the camera.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>The primary and secondary recorders are online. The primary recorder has a valid connection to the camera, and the status of the connection between the secondary recorder and the camera is unknown because redundancy is not enabled.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>The primary recorder is online and has a valid connection to the camera. The secondary recorder is offline.</td>
</tr>
<tr>
<td><img src="image4" alt="Icon" /></td>
<td>The primary recorder is offline. The secondary recorder is online, but does not have a valid connection to the camera.</td>
</tr>
<tr>
<td><img src="image5" alt="Icon" /></td>
<td>Either the camera, both recorders, or all three devices are logically marked offline.</td>
</tr>
</tbody>
</table>

**Video Monitoring Features**

The following features are available for video monitoring.

**Buffering Streaming Video**

Buffering of live and recorded video reduces the amount of network bandwidth used by buffering the video on the client machine for playback. Video may be viewed multiple times from the client rather than requesting the video from the video recorder repeatedly.

This feature enhances live video mode by allowing the user to review live video that has been cached without switching to recorded video. The live video toolbar now displays a slider which can be used to navigate the cached video. The current time of the video is displayed in the toolbar. The live video cache retains a maximum of 10 minutes. The maximum size per cached video stream is 50 MB of RAM. Live video can be paused, resumed, slowed, or accelerated. Live video play will resume if video is paused or slowed down until it reaches the beginning of the cache or if video is accelerated to the current time.

Buffering of recorded video occurs during playback. During video playback, recorded video is cached in 10 minute increments.

To turn on the buffering of live and/or recorded video on a per workstation basis, add the following lines to the [DigitalVideo] section of the ACS.INI file:
Video Monitoring Features

- To turn on live: BufReader0=1
- To turn on recorded: BufReader2=1

To turn buffering back off, remove the line(s) above or set the value equal to 0.

Browser-based VideoViewer

An alternative to using the video player is to use the browser-based VideoViewer. The browser-based VideoViewer has some enhanced feature capabilities that are not available in Alarm Monitoring. Some of these features include:

- More flexible recorded video viewing options
- Robust layout manipulation
- Better joystick control with the use of buttons

For more information about these features, refer to the VideoViewer (Browser-based) User Guide.

The browser-based VideoViewer can be launched from Alarm Monitoring. The Use browser-based VideoViewer option located in the right-click menus of supported video devices can be used to enable this feature on a per workstation basis. A check mark next to the menu option indicates that the feature has been enabled. Once the Use browser-based VideoViewer option has been enabled, all manual requests for live and recorded video will be displayed in VideoViewer.

To use the browser-based VideoViewer, the Web Application Server must be fully installed and configured. For more information, refer to the Installation Guide.

Camera Lookup

Camera lookup is used to locate a specific camera or multiple cameras by name. The search permissions can be configured to include only the current monitor zone or the entire system. To perform a camera lookup, right-click the monitor zone or camera device group in Alarm Monitoring and select “Camera lookup...” Searches initiated from the monitor zone will have the results highlighted in the System Hardware Tree and searches initiated from a camera device group will have the results highlighted in the Device Groups window. Searches that return results outside of the current monitor zone or device group will be added to the monitor zone or device group.

The extent of the search is limited by a user permission on the Users > Monitor Permission Groups > Video sub-tab. To enable a user group to search for cameras across the entire system, select the Camera lookup includes all monitor zones check box. In segmented systems, users must have segment access to the segment in which the cameras video recorder resides for it to appear in the search results.

When a search is performed, the Camera Lookup dialog is displayed. The Camera Lookup dialog message indicates whether the search will be performed in the current monitor zone or across the entire system. The search is performed by entering a portion of the camera name, wildcard characters (*) are not used. For example, a search for “hall” would return cameras named “Hallway”, “Main hall”, and “Hall stairwell” if they existed in the system.

If a single camera is found it is highlighted in the System Hardware Tree or Device Groups window. If multiple cameras are found that match the string entered, they are displayed in the Select Cameras dialog. Multiple cameras can be selected for addition to the monitor zone by placing a check mark beside each camera. The first selected camera will be highlighted and additional selected cameras will be added to the monitor zone if they are not already included. This addition to the monitor zone is temporary and restricted to the current Alarm Monitoring session, camera additions are not saved per user or workstation.
**Two-way Audio**

Two-way audio enables communication between a monitoring workstation and a camera equipped with a microphone and speakers. A workstation can communicate with a single device or multiple devices simultaneously. A microphone or a pre-recorded file can be used to send audio to the device.

Audio quality is dependent on the quality of the hardware. The two-way audio streams are retrieved by the client directly from the camera. Audio sent to the camera from the client is not captured by the video recorder and cannot be recorded.

Two-way audio is enabled on the Audio tab of the Camera form in System Administration. If the selected camera does not support two-way audio, the Allow Two-Way Audio check box will be grayed out. Two-way audio devices may support full or half-duplex. Full duplex allows simultaneous two-way communication, while half-duplex allows communication in one direction at a time. The Two-Way Audio check box on the Users > Monitor Permission Groups > Video sub-tab determines user permissions for the feature.

Two-way audio is controlled by the Two-Way Audio Communication dialog. This dialog can be launched from the right-click menu of a supported camera in the System Status Tree in Alarm Monitoring or from the Play menu in the video player or VideoViewer. If the camera is either not configured or not supported for two-way audio, the option will be grayed out. All devices are controlled from the same Two-Way Audio Communication dialog. Each device can be controlled individually or multiple devices can be controlled simultaneously by selecting the check boxes of the devices and using the Multiple Selection Controls portion of the dialog.

**Note:** Two-way audio is not available if the camera is in MPEG4 mode.

**Two-way Audio Communication Dialog Fields**

**Device name and status**

The name of the device is displayed with each control with the status of the device in parenthesis. Statuses include:

- Active - The device is currently being controlled.
- Inactive - There is a connection to the device, but the controls are not currently in use.
- Connecting - An attempt is being made to connect to the device.
- Communication error - There is a problem connecting to the device.

**Talk/End Talk**

This button begins and ends transmission from the monitoring workstation to the camera using a microphone. The [Talk] button changes to [End Talk] while the connection is active. This button is disabled under the following conditions:
Video Monitoring Features

- A file is currently being sent.
- A connection is being established to the device.
- The camera supports only half-duplex mode and [End Listen] is currently active.

**Listen/End Listen**
This button begins and ends transmission from the camera to the monitoring workstation. The [Listen] button changes to [End Listen] while the connection is active. This button is disabled under the following conditions:
- A connection is being established to the device.
- The camera supports only half-duplex mode and [End Talk] or [End Send File] is currently active.

**Send File/End Send File**
This button begins and ends transmission from the monitoring workstation to the camera using an audio file. The [Send File] button changes to [End Send File] while the file is being transmitted.

When [Send File] is pressed, a dialog allows you to browse for an audio file. Only the .WAV 8kHz 16-bit PCM file format is supported. To cancel the file before it is complete, press [End Send File]. This button is disabled under the following conditions:
- [End Talk] is currently active.
- A connection is being established to the device.
- The camera supports only half-duplex mode and [End Listen] is currently active.

**Reconnect**
This button is displayed when the connection to the camera is lost or cannot be established. When clicked, an attempt will be made to reconnect to the camera.

**Device check boxes**
Select the check box for each device that you wish to control using the Multiple Selection Controls portion of the dialog.

**Close button (Red X)**
Each device control includes a close button (red X). Pressing this button closes the connection to the device and removes the control from the dialog. If the dialog contains only one control, the dialog is closed.

**Multiple Selection Controls**
These buttons are used in conjunction with the device check boxes to control multiple devices simultaneously from one set of controls.

**Select all**
Select this check box to select all devices for use with the Multiple Selection Controls. Deselect this check box to clear the check boxes for all devices.

**Video Tour Options Dialog Fields**

**Default Interval (sec)**
This value is used differently in on-the-fly and custom tour functionality. For on-the-fly tours, this is the time delay that applies to all the tour steps which is similar to the previously used Video Interval option. For custom tours, this value is used as the default for the Delay edit option during custom tour configurations.
Video Monitoring Procedures

Use the following procedures for video monitoring.

Launch Video (Live/Recorded) From a Camera

1. To launch video in the VideoViewer complete one of the following:
   - Double-click a camera.
   - Drag and drop a camera, camera device group or recorder into the display window or Video Player. If you drag and drop a device group or recorder into the Video Player, the first camera in the group that was added to the database displays.

2. To launch video in Alarm Monitoring complete one of the following:
   - In an alarm window right-click an alarm with associated video and select Launch Video. Recorded video will be launched with the start time of the active alarm, including pre-roll if configured.
   - In a map or System Status window right-click a device icon and select Launch Video.
   - In the Device Group window right-click a camera icon and select Launch Video.
   - In the Video Monitoring window double-click an online camera or right-click a camera icon and select Launch Video.
   - Drag and drop a camera, camera device group or recorder into the Video Player. This launches ALL of the video cameras in that particular group or recorder (up to 32 cameras at once).

3. To switch to live video in the Video Player or VideoViewer, select Live from the Play menu.

4. To switch to recorded video in the Video Player or VideoViewer, select Recorded from the Play menu.

Launch Video From a Specific Source

Depending on your configuration there may be more than once source available to launch video for IP cameras from. These sources are available from the right-click menu of individual cameras. Sources that are not configured in your system will be disabled in the right-click menu.

Note: To launch video from a failover recorder, video failover must be configured for the IP camera in System Administration. For more information, refer to “Video Recorder Failover and Redundancy” in the System Administration User Guide.

To launch video from a specific source, select one of the following options from the right-click menu of the IP camera:

- **Launch Video From > Primary Recorder** - used to launch live video from the main LNVR configured for the camera.
Video Monitoring Procedures

- **Launch Video From > Failover Recorder** - used to launch live video from the secondary LNVR configured for the camera.
- **Launch Recorded Video From > Primary Recorder** - used to launch recorded video from the main LNVR configured for the camera.
- **Launch Recorded Video From > Failover Recorder** - used to launch recorded video from the secondary LNVR configured for the camera.
- **Launch Recorded Video From > Archive Server** - used after video has been archived to launch recorded video from the archive server.

**Monitor Video of a Specific Camera**

To monitor video of a specific camera in Alarm Monitoring complete one of the following:

- In the Video Monitoring window double-click an online camera to view live video.
- In an alarm window, map or System Status window right-click a device icon and select *Launch Video* to view live or recorded video.
- In the Device Group window right-click a camera icon and select *Launch Video* to view live or recorded video.
- In the Video Monitoring window double-click an online camera or right-click a camera icon and select *Launch Video*.
- Drag and drop a camera into the Video Player.

**Toolbar Shortcut**

- If the Video Player is in matrix view, select Single View from the Video Layout toolbar button. Click the Previous Camera or Next Camera toolbar buttons to view a specific camera.
- In the Video Player select *Camera* from the *View* menu. A sub-menu lists the currently displayed cameras. Select the camera of your choice.

**About Surveillance-Only Cameras**

Surveillance-only cameras support live video only, they cannot record or playback video, whereas IP (Internet Protocol) cameras can. IP cameras are directly connected to the network with their own IP address. They do not need to be connected to a computer 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.

**Send Video**

The Live Video Recipients List dialog can be used to send video from a video channel to an external client that supports that particular recorder type. Currently supported external clients are SkyPoint and Prism clients.

To use this feature, you must perform one of the following configurations:

- If you have an external client other than OnGuard, you must add this external client to OnGuard. For more information, refer to “Configure Send Video with SkyPoint Base Server” in the System Administration User Guide.
- If you do not have an external client on your system, recipients for send video are configured on the NetDVMS and imported into OnGuard. For more information, refer to “Configure Send Video with NetDVMS” in the System Administration User Guide.
The external clients application must also be open on the client with at least one cell configured to receive push video.

The lists of recipients can come from multiple services and are combined.

To send video to recipients complete the following steps:

1. Open the Live Video Recipients List dialog in Alarm Monitoring by one of the following methods:
   - Right-click a camera in the Hardware Tree and select **Send Video To**.
   - From the Video Player, select **Options > Send Video**.
   - Right-click an alarm with associated video and select **Send Video To**.

2. To search the recipient list:
   - Select the **Search Recipient by Type Filter** radio button and select a server type from the drop-down or
   - Select the **Search Recipient by Name** radio button, specify a search term in the text box, and click [Find].

3. Select the recipients from the listing window and click [OK]. To select more than one recipient, hold <Ctrl> and click each recipient from the list.

4. Click [OK] to push video to the selected recipients.

---

**Event Configuration/Search Dialog**

The Event Configuration/Search dialog is used to:

- Configure event parameters for real-time LNVR video processing and alarm generation. For detailed IntelligentVideo Event information, refer to the IntelligentVideo User Guide.
- 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.
Event Configuration/Search Dialog

- Search LNVR or LDVR 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.

Note: 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 Configuration/Search Dialog - Menus

<table>
<thead>
<tr>
<th>Menu Name</th>
<th>Menu Options</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Menu Select Event</td>
<td>Enables you to select the event for which the current video source will be analyzed.</td>
<td></td>
</tr>
<tr>
<td>Note: 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 the Select Event sub-menu option will not display.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen Output</td>
<td>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 that a checkmark displays beside this sub-menu option.</td>
<td></td>
</tr>
<tr>
<td>Load/Save Configuration</td>
<td>Allows you to save the current configuration and load it at a later time for the same type of event.</td>
<td></td>
</tr>
<tr>
<td>Copy/Paste Configuration</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
### Event Configuration/Search Dialog - Menus (Continued)

<table>
<thead>
<tr>
<th>Menu Name</th>
<th>Menu Options</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Player Menu</td>
<td>Switch to Recorded/Live</td>
<td>Enables you to switch to and from recorded and live video.</td>
</tr>
<tr>
<td></td>
<td>Select Start/End Times</td>
<td>Displays a dialog where you can select the start and end times of a recorded video search.</td>
</tr>
<tr>
<td></td>
<td>Export Frame</td>
<td>Allows you to export the current frame into a picture file. Supported image formats are BMP, JPEG, GIF, TIFF, and PNG.</td>
</tr>
<tr>
<td></td>
<td>Play</td>
<td>Starts/resumes video playback. This command is not visible when video is playing.</td>
</tr>
<tr>
<td></td>
<td>Pause</td>
<td>Pauses playback. When video play is resumed, it continues from where it was temporarily stopped. This command is visible only when video is playing.</td>
</tr>
<tr>
<td></td>
<td>Stop</td>
<td>Stops playback and rewinds the video to the beginning.</td>
</tr>
<tr>
<td>Search</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Zoom</td>
<td>Enables you to set pre-defined (50%, 100%, and 200%) zoom levels for the video player.</td>
<td></td>
</tr>
<tr>
<td>Frame Rate</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

### 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
Video Monitoring

- Play, pause, and stop recorded video
- Play the video at an accelerated rate by using the search button

![Playing... 09/14/05 14:04:38](image)

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.

![Live Video... 09/16/04 13:23:48](image)

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. 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.

![Alert status graph](image)

Time Range

Select the duration of time used by the graph.
Event Configuration/Search Dialog Procedures

Use the following procedures in this dialog.

Open the Event Configuration/Search Dialog

The Event Configuration/Search dialog can be opened using the Video Processing form or IntelligentVideo form (in System Administration) or using the Video Search menu option (in Video Player).

Level

The current level of change. Levels range from 0 to 100. The first and last frames of an event must have a value equal to or greater than the specified level, to be included in the search results.

<table>
<thead>
<tr>
<th>Output</th>
<th>Value</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm State</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level</td>
<td>100</td>
<td>0</td>
<td>100</td>
</tr>
</tbody>
</table>

History

Displays the history of the level of change.

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 event configuration is modified, this button will be enabled and allow the user to apply configuration changes to the IntelligentVideo engine.
Using the Video Processing or IntelligentVideo Form

1. Open the Video Processing or IntelligentVideo form from System Administration:
   • For IntelligentVideo events:
     1) From the Video menu, select IntelligentVideo. The IntelligentVideo folder opens.
     2) Click the IntelligentVideo Events tab.
   • For Video Processing events:
     3) From the Video menu, select Digital Video. The Digital Video folder opens.
     4) Click the Video Processing tab.

2. Select (place a checkmark beside) the appropriate camera.

3. Click [Modify].

4. 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. Follow the procedures to Launch Video (Live/Recorded) From a Camera on page 86. Verify the recorded video is playing in the Video Player.

   Toolbar Shortcut

   2. Click the Video Search toolbar button or from the Control menu select Video Search. The Event Configuration/Search dialog displays.

Configure Event Properties

When you configure event properties, you define the parameters that make up an event. For example, duration time and object size are event properties for the “Left Object” 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 93.

2. If you opened the Event Configuration/Search dialog using the Video Player, select the event type from the Event menu.

3. Set the region of interest. For more information, refer to Set Region of Interest on page 95.

4. Set the event properties. For more information, refer to the IntelligentVideo Events chapter in the IntelligentVideo User Guide.

5. If necessary, configure event parameters that apply to the video channel itself. For more information, refer to Video Channel Configuration Dialog on page 97.
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 Dialog on page 88.
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.
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.

### Video Search Performance Requirements

A fast network, 100 Mbps or greater, is recommended between the site where video is located and the site where the computer running the Video Player is located. A fast network is recommended because video is analyzed/searched on the client side, therefore the faster video can be transmitted from the server side, the faster the search will be.

The hard drive speed on the server side must be able to support the number of clients using the server. Clients include Video Players and archive servers.

A fast CPU on the client computer is also recommended. Generally, when the network and server side hard drive are fast enough, the CPU on the client side can be the bottleneck. A Pentium III based computer is required although a Pentium IV computer is recommended.

### Search Video/Audio

You can search video and audio using the Video Player or Event Configuration/Search dialog. To search video using the Video Player, simply verify recorded video is playing and select the start/end date. However, the Event Configuration/Search dialog enables you to perform detailed searches quickly. Complete the following to search video 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 93.

2. If you opened the Event Configuration/Search dialog using the Video Player, select the event type from the **Event** menu.

3. From the **Player** menu select **Select Start/End Times**. The Date / Time window opens. Enter the desired date and time ranges you wish to search and click [OK].

**Note:** You can also set the start/end date by selecting **Options > Set Start/End Date** in the video player.

4. From the **Player** menu select **Frame Rate**.

5. Set the configuration parameters for the event or load a previously saved set of channel configuration parameters. For more information on event configuration parameters, refer to the IntelligentVideo Event chapters in the IntelligentVideo User Guide. For more information on
audio events, refer to IntelligentAudio on page 513. For more information on channel configurations, refer to Video Channel Configuration Dialog on page 97.

6. Click the search toolbar button. Events that meet the configuration parameters display in the Alarm History pane.

**View Search Results**

There are several ways to view the recorded video associated with the video search results.

From the Event Configuration/Search dialog:

- Click any part of the graph, in the Event Feedback pane.
- Double-click a thumbnail or listed event, in the Alarm History pane.

**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 increased 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. 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.

Open the Video Channel Configuration Dialog
The Video Channel Configuration dialog can be opened using the IntelligentVideo Events form (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 93.
2. Click [Channel Configuration] (located on the lower right side of the window). The Video Channel Configuration dialog opens.

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. 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 98.
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.
7. Click [OK].

**Remote Monitor**

Remote Monitor (RM), commonly referred to as “camera call-up”, is a video monitoring application that can be run on any PC with or without OnGuard installed. Configuration is performed in System Administration. The RM application behaves as a slave to the Alarm Monitoring application which is used to send video commands allowing the user to:

- Launch video on the RM or Remote Monitor Group (RMG).
- View status of the RMs in the System Hardware Tree and the RMGs in the Device Group window.
- Send matrix mode, camera selection, and video playback commands to the RM.
- Mute audio.
- Drag and drop cameras onto the RM or RMG icon to start live video playback.
- Drag and drop alarms with associated video onto the RM or RMG icon to start recorded video playback.
- Activate Video Quality Enhancement algorithms for the RM or individual camera channels.
- Launch a local monitor window on the Alarm Monitoring workstation to send commands performed in the window to the RM.

**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.

**Note:** 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.

**Add Cameras to a Remote Monitor**

Cameras can be added via multiple drag and drop operations.
The source of the camera can be one of the following:

- Camera icon in the System Status Tree
- Alarm icon that has associated video from the Alarm view

The target of the drag and drop operations can be one of the following:

- RM icon in the hardware tree or device group view
- RMG icon in the device group view
- Local monitor window

Cameras that have been added to a Remote Monitor appear in the System Status Tree below the RM and are referred to as video cells or Remote Monitor Cells (RMC). RMGs are displayed in the Device Group window with lists of the RMs that belong to each group. Cameras added to RMGs are added to each RM that belongs to that group.

- - Remote Monitor
- - Remote Monitor Cell
- - Remote Monitor Group

**Remote Monitor Right-click Options**

Commands are available for RMs and RMCs through a right-click menu and drag and drop functionality. Right-click options specific to Remote Monitors are listed in the table below.

**Launch Video (RM)**
Launches the local monitor window in Alarm Monitoring.

**Launch Video (RMC)**
Launches video on the RM and the local monitor window in Alarm Monitoring.

**Download Database (RM)**
Synchronizes the RM with the camera channels assigned in Alarm Monitoring.

**Remove All (RM)**
Removes all video from the RM.

**Remove (RMC)**
Removes the video cell from the RM.

**Select (RMC)**
In matrix view, changes to single player mode with the selected video cell.

**Matrix**
Switches the RM to matrix view.

**Single**
Switches the RM to single player mode.

**Next**
In single player mode, selects the next video cell in the list.
Prev
In single player mode, selects the previous video cell in the list.

Live
Changes to live video on each video cell in the RM.

Recorded
Changes to recorded video on each video cell in the RM.

Pause
Pauses the video playback on each video cell.

Play
Resumes the video playback on each video cell.

Stop
Stops the video playback on each video cell.

Frame Advance
Advances one video frame on each video cell.

Fast Forward End
Fast forwards to the end on each video cell.

Mute Audio
Mutes the audio on the RM or video cell.

Unmute Audio
Turns mute off for the RM or video cell.

VQE
Contains several options for the Video Quality Enhancement (VQE) algorithms. For more information, refer to Video Quality Enhancements on page 111.

Activate De-Interlacing (RM)
Select this menu item to turn De-interlacing on for the RM.

De-Interlacing (RMC)
Select this menu item to turn De-interlacing on for the video cell. A check box next to this menu item indicates that the De-Interlacing algorithm is in use on the video cell.

Activate Sharpener (RM)
Select this menu item to turn Sharpener on for the RM.

Sharpener (RMC)
Select this menu item to turn Sharpener on for the video cell. A check box next to this menu item indicates that the Sharpener algorithm is in use on the video cell.

Activate Fog Removal (RM)
Select this menu item to turn Fog removal on for the RM.
Fog Removal (RMC)
Select this menu item to turn Fog removal on for the video cell. A check box next to this menu item indicates that the Fog Removal algorithm is in use on the video cell.

Clear All
Select this menu item to turn off all of the VQE algorithms for the RM or video cell.

Options
Select this menu item to open the Video Quality Enhancement Configuration Dialog.

Local Monitor Window in Alarm Monitoring
The Local Monitor Window (LMW) is a mirror of the RM that can also be used to send commands from Alarm Monitoring. To open the LMW, right-click on the RM or RMC in the System Status Tree and select Launch Video. If the LMW is opened from an RMC, the RM will switch to single view and display the selected video cell.

The following commands will be sent to the RM while manipulating video in the LMW:

• Remove selected cameras. This can be done by selecting Remove Video from the right-click menu in matrix mode, by selecting Remove Video from the Control menu, or by pressing the delete key.
• Switch to matrix view or single player view.
• Select camera, move to the next camera, and move to the previous camera in single player view.
• Switch between live and recorded video.
• Change recorded video time frame.
• Pause, resume, stop, frame advance, and fast forward to end commands.
• Mute audio, when selected from the right-click menu. If audio is muted in the LMW by clicking the speaker icon, this command will not be sent to the RM.
• Activate Video Quality Enhancement (VQE) algorithms.

Remote Monitor Application
The Remote Monitor Application (RMA) behaves as a slave to Alarm Monitoring and does not support any video commands. The user has the following commands available:

• Launch and exit the application. Upon exit, the RMA looses video cell information. When the RMA comes back online, it must be synchronized via the Download Database command in Alarm Monitoring.
• Move and resize the main window.
• Close the application window.
• Open the window and exit the application by right-clicking the application’s icon in the system tray.
• Mute audio on one or more cameras by clicking the speaker icon.
• Turn on and off automatic window launch via the Auto launch on command in the Options menu. When this setting is enabled, the RMA window will open to the previous position when the RM receives a matrix mode, camera selection, or video playback command.
• Activate full screen mode by selecting Full Screen from the Options menu. To deactivate full screen mode, press <Esc>. You can also toggle full screen by pressing <Alt> + <Enter>.
• Change the TCP/IP connection port.
Remote Monitor

Change the Remote Monitor TCP/IP Port

The Remote Monitor TCP/IP port is used by OnGuard to communicate with the Remote Monitor. The port number in the Remote Monitor application must match the port number defined in System Administration.

1. In the Remote Monitor application, select the Connection > Settings menu option.
2. The Connection Settings window is displayed.

   a. Enter the new port number in the TCP/IP Port field.
   b. Click [OK].

Application Profiles

Users of the Remote Monitor application can save the current settings as a profile for later use. Settings such as TCP/IP port number, window position, always on top, launch on command, and full screen mode are part of a Remote Monitor application profile.

Note: Remote Monitor must be run by a user with Administrative permissions to save or remove profiles.

Save a Remote Monitor Profile

1. In the Remote Monitor application, select the Profile > Save As menu option.
2. The Save Profile window is displayed.

   • To create a new profile, select the Create New radio button and enter a Name.
• To change an existing profile, select the **Overwrite Existing** radio button and highlight the profile you want to update.

3. Click [OK] to save the profile.

**Load a Remote Monitor Profile**

1. In the Remote Monitor application, select the **Profile > Load** menu option.
2. The Load Profile window is displayed.

![Load Profile Window](image)

   a. Select the profile you want to load.
   b. Click [OK].

**Remove a Remote Monitor Profile**

1. In the Remote Monitor application, select the **Profile > Save As** menu option.
2. The Save Profile window is displayed.

![Save Profile Window](image)

   a. Select the **Overwrite Existing** radio button.
   b. Highlight the profile you wish to delete.
   c. Click [Remove].
3. Click [OK] to close the Save Profile window.
Chapter 8: Video Player

Video Player

The Video Player performs the following functions:

- Displays live or recorded video from one camera
- Displays live or recorded video from a group of cameras successively
- Displays video from a group of cameras or a recorder simultaneously.
- Displays recorded video associated with a video search
- Enables you to pan, tilt and zoom recorded and live video

The Video Player is displayed by right-clicking an alarm, device, camera or camera device group and selecting Launch Video.

Note: Refer to the Video Player Status Bar Table on page 107 for the descriptions of the status bar components, A-F.
### Video Player Menu and Toolbar Buttons Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Toolbar button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play menu</td>
<td></td>
<td>Contains the following menu options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Live:</strong> Plays live video from one or several cameras depending on the view settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Recorded:</strong> Plays recorded video for the selected camera(s).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>File:</strong> Plays video clips from a file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> A checkmark displays beside the option that is active.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Load Layout:</strong> Restore a previously saved video matrix layout.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Save Layout:</strong> Save the current video matrix view as a new layout.</td>
</tr>
<tr>
<td>Control menu</td>
<td></td>
<td>Contains several options to play, pause and stop video as well as advance video, adjust playback speed, search video, mute audio and remove cameras from the Video Player window.</td>
</tr>
<tr>
<td>Options menu</td>
<td></td>
<td>Contains options to load video files, set start/end times to view recorded video, export video to a file, capture images from video, create video events, modify video performance (frame rate, quality, and video acceleration), and configure PTZ tours and presets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Send Video menu option is used to send video from NetDVMS cameras to a SkyPoint client. For more information, refer to Send Video on page 87.</td>
</tr>
<tr>
<td>View menu</td>
<td></td>
<td>Contains options to change how cameras views are displayed, IntelligentVideo Overlay, and Video Quality Enhancement options.</td>
</tr>
<tr>
<td>Play button</td>
<td><img src="image" alt="Play" /></td>
<td>Plays recorded video.</td>
</tr>
<tr>
<td>Pause button</td>
<td><img src="image" alt="Pause" /></td>
<td>Pauses or temporarily stops playing recorded video. The video will continue from where it temporarily stopped when the play button is clicked.</td>
</tr>
<tr>
<td>Stop button</td>
<td><img src="image" alt="Stop" /></td>
<td>Stops playing recorded video and resets the player to the beginning of the video.</td>
</tr>
<tr>
<td>Frame Advance button</td>
<td><img src="image" alt="Frame Advance" /></td>
<td>Advances video one frame at a time.</td>
</tr>
<tr>
<td>Fast Forward End button</td>
<td><img src="image" alt="Fast Forward End" /></td>
<td>Advances (fast forwards) video to the last frame.</td>
</tr>
<tr>
<td>Previous Camera</td>
<td><img src="image" alt="Previous Camera" /></td>
<td>Displays the previous camera view. This feature only applies when you have opened multiple images and the Video Player is in single view mode.</td>
</tr>
<tr>
<td>Next Camera</td>
<td><img src="image" alt="Next Camera" /></td>
<td>Displays the next camera view. This feature only applies when you have opened the Video Player so that you can view multiple images and you are currently in single view.</td>
</tr>
<tr>
<td>Video Layout</td>
<td><img src="image" alt="Video Layout" /></td>
<td>Displays the selected visual matrix of video cells. Options include single view, matrix view, and static templates (1x1, 2x2, 3x3, 4x4, 13+1, 1+5, and 5+1).</td>
</tr>
</tbody>
</table>
Activate PTZ Enables PTZ commands for supported cameras. For more information, refer to Pan, Tilt, and Zoom on page 119.

Activate Digital PTZ Enables digital zoom for PTZ cameras.

Display window Displays live or previously recorded video.

Status indicators NetDVMS cameras have 4 status indicators in the upper right-hand corner of the display window. The status indicators have the following definitions:

- Green - live video
- Blue - motion detected
- Red - recording
- Yellow - an event has occurred for the camera

Status bar For information on the status bar please refer to Video Player Status Bar Table on page 107.

<table>
<thead>
<tr>
<th>Field</th>
<th>Toolbar button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate PTZ</td>
<td>![PTZ Icon]</td>
<td>Enables PTZ commands for supported cameras.</td>
</tr>
<tr>
<td>Activate Digital PTZ</td>
<td>![Digital PTZ Icon]</td>
<td>Enables digital zoom for PTZ cameras.</td>
</tr>
<tr>
<td>Display window</td>
<td></td>
<td>Displays live or previously recorded video.</td>
</tr>
<tr>
<td>Status indicators</td>
<td></td>
<td>NetDVMS cameras have 4 status indicators in the upper right-hand corner of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the display window. The status indicators have the following definitions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Green - live video</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Blue - motion detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Red - recording</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Yellow - an event has occurred for the camera</td>
</tr>
</tbody>
</table>

Video Player Status Bar Table

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Camera Icon]</td>
<td>When live video is playing the status bar displays the camera name.</td>
</tr>
<tr>
<td>If an LNVR is offline, the video player can connect directly to an IP camera to display live video. A direct connection to the IP camera is indicated in the video player status bar by a ![Camera Icon] icon. If failover is configured, the video player can retrieve video from the secondary recorder. The ![Camera Icon] icon is used to indicate that video is coming from the secondary, or failover, recorder.</td>
<td></td>
</tr>
<tr>
<td>If video quality enhancements are in use, they are indicated in the video player status bar by a ![Camera Icon] icon.</td>
<td></td>
</tr>
<tr>
<td>When recorded video is playing the status bar contains two arrow heads ![Camera Icon]. You can click the arrow heads to change the information displayed to any of the following:</td>
<td></td>
</tr>
<tr>
<td>- Camera name</td>
<td></td>
</tr>
<tr>
<td>- Video start date and time</td>
<td></td>
</tr>
<tr>
<td>- Video start date/time and end date/time</td>
<td></td>
</tr>
</tbody>
</table>
Video Player Status Bar Table (Continued)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
</table>
| B      | Move the slider back and forth to view video at different dates/times. You do not need to pause or stop video to use the video display slider.  
  Note: Cameras configured with an LNVR recorder display different colors in the slider for different types of recorded video.  
  - Red - video is not available (e.g. a download was performed, LNVR was disconnected or restarted)  
  - White - video is not being recorded (e.g. time lapse recording)  
  - Green - video is being recorded (e.g. continuous recording or time lapse recording)  
  - Black - time synchronization (e.g. a third-party application has updated the time on the LNVR)  
  - Gray - video has not been cached on the client yet |
| C      | Video start time. Use this feature to adjust your video search. |
| D      | Determines how fast the video is played as well as searched. Using the cursor click near the minus symbol to slow the video down or click the plus symbol to speed the video up. You can also adjust the speed by clicking and dragging the speed bar arm. |
| E      | Video end time. Use this feature to adjust your video search. |
| F      | Set the volume level for the camera with audio recording enabled. Click the icon to toggle mute. A red X will appear when the audio is muted. |

Aspect Ratio

By default the aspect ratio of video in the Video Player is pan and scan. In this mode the video will occupy the entire cell and disregard the camera's default aspect ratio.

To keep the default aspect ratio of the camera you must edit the MatrixWideScreenMode parameter under the [DigitalVideo] heading of the ACS.ini file to be: MatrixWideScreenMode=3.

This will default the aspect ratio to that of the camera. To change the aspect ratio back to pan and scan change the MatrixWideScreenMode parameter to be: MatrixWideScreenMode=4.

Daylight Saving Time

To search video that was recorded the hour before or after the Daylight Saving Time changeover, you must perform two searches instead of one. For example, in the Eastern Standard Timezone the Daylight Saving Time changeover occurs at 2:00 a.m. To view video that was recorded between 1:00 a.m. and 3:30 a.m., perform two searches. For the first search, specify 1:00 a.m. for the start time and 1:59:59 for the end time. For the second search, specify 3:00:01 a.m. for the start time and 3:30 a.m. for the end time. Use this same technique when exporting video recorded during the changeover time.

Attempting to play or export a continuous video clip with a start time before 2:00 a.m. to an end time after 3:00 a.m. is not recommended and may result in undesired playback behavior. For this reason, search and/or export recorded
video before the Daylight Saving Time changeover separate from video after the changeover.

**Troubleshooting**

If you receive the message: “The end time must not be before the start time.” set the End time to 1:59.59 a.m. not 2:00:00 a.m.

If you receive the message: “The time requested is not available on the Video Recorder, and could not be located on the Video Archive Server.” set the Start time to 3:00:01 a.m. not 3:00:00 a.m.

**Customize Overlay Information Dialog**

The Customize Overlay Information Dialog displays when you export video in an “.ASF” format and you click [Customize]. For more information, refer to Customize Overlay Information Dialog on page 508.

![Customize Overlay Information Dialog](image)

**Performance Dialog**

Adjustments to the Video Player can be made to enhance performance by limiting the frame rate, decompression, video acceleration, and edge enhancement. The Performance dialog is displayed by selecting **Options > Performance** from the Video Player window. Settings are configured and stored for the monitoring station and apply to both live and recorded video. Any changes to performance settings take effect after the Video Player is restarted.
Video Player - Performance dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame rate limit (LNVR only)</td>
<td>Limit the frame rate displayed by the Video Player. Useful for remote clients that have limited bandwidth.</td>
</tr>
<tr>
<td>Play key frames only</td>
<td>Enable to throttle out the P-frames and only play the I-frames.</td>
</tr>
<tr>
<td>Decompression Quality (LDVR-408 and LDVR-444 only)</td>
<td>Determines the quality of the video decompression which influences the size of the image displayed in the Video Player. The lowest decompression setting produces a smaller image and requires fewer resources from the client computer.</td>
</tr>
<tr>
<td>Edge Enhancement Filter (LDVR-408 and LDVR-444 only)</td>
<td>Determines whether the LDVR decoder should favor smooth images or detail. Lower values produce smoother images, but lose some small details. Higher values produce a grainy image, yet emphasize and sharpen details.</td>
</tr>
<tr>
<td>Video Acceleration</td>
<td>Used for troubleshooting problems displaying video related to the video card or device drivers. Full acceleration utilizes the video card, thus freeing the computer CPU and memory for other tasks. Additionally, Windows Display Properties has a Hardware Acceleration setting on the Troubleshoot tab of Advanced Settings that may be used for troubleshooting. Note: Some video cards and device drivers may produce varying results. Adjust the value to each level to find the one that generates the desired effects.</td>
</tr>
<tr>
<td>OK</td>
<td>Save settings and return to the Video Player window.</td>
</tr>
<tr>
<td>Note:</td>
<td>You must close the Video Player for the changes to take effect.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Close the Performance dialog without saving changes.</td>
</tr>
</tbody>
</table>
Video Quality Enhancements

The Video Quality Enhancement (VQE) algorithms are used to enhance video viewing quality. VQE algorithms can be configured in Alarm Monitoring or Remote Monitor.

The Video Quality Enhancement Configuration dialog is displayed by selecting View > VQE Options from the Video Player menu. VQE can also be activated using shortcuts for each algorithm in the Video Player menu in either single view or matrix view.

Note: To cancel all VQE settings, select View > Clear All VQE from the Video Player menu.

De-interlacing

The De-interlacing algorithm can be used to eliminate blurriness caused when objects are in motion. There are no configurable parameters for De-interlacing.

Sharpener

The Sharpening algorithm is used to enhance the video quality in circumstances in which the camera view may be blurred. The level of enhancement is configurable.

Fog Removal

The Fog Removal algorithm is designed to enhance the video quality when rain or fog is in the camera view. Rain and fog can decrease the contrast of video obscuring object details. The level of enhancement is configurable and can also be set to automatic. There is also an optional Noise Filter that can be configured by selecting the check box.
Video Player - Video Quality Enhancement Configuration Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>De-interlacing</td>
<td>Select this check box to turn De-interlacing on. Note: De-interlacing can also be activated by selecting View &gt; Activate De-Interlacing from the Video Player menu.</td>
</tr>
<tr>
<td>Sharpener</td>
<td>Select the check box to turn Sharpener on. Adjust the slider the customize the level of sharpening. Note: Sharpener can also be activated by selecting View &gt; Activate Sharpener from the Video Player menu.</td>
</tr>
<tr>
<td>Fog removal</td>
<td>Select the check box to turn Fog removal on. Adjust the slider to customize the level or select the Auto check box to automatically configure level of the algorithm. Note: Fog removal can also be activated by selecting View &gt; Activate Fog Removal from the Video Player menu.</td>
</tr>
<tr>
<td>Noise Filter</td>
<td>Select this check box to reduce the noise present in the video stream. This feature is used in combination with the Fog Removal algorithm.</td>
</tr>
<tr>
<td>OK</td>
<td>Save settings and return to the Video Player window.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Close the Video Quality Enhancement Configuration dialog without saving changes.</td>
</tr>
<tr>
<td>Apply</td>
<td>Save settings and view the effects in the Video Player window without closing the Video Quality Enhancement Configuration Dialog.</td>
</tr>
<tr>
<td>Help</td>
<td>View help for this topic.</td>
</tr>
</tbody>
</table>

**Video Player Procedures**

**Export Video to a File**

Video can be exported to a file using the Video Export dialog from the Video Player. For more information, refer to Export Video to a File on page 509.

**Load and View a Video File**

1. Display the Video Player. For more information, refer to Video Player on page 105.
2. Select Load File from the Options menu.
3. The Open window displays. Select the correct ".info" file, and click [Open]. The recorded video automatically plays.
4. To replay the video file click the Stop toolbar button and then click the Play toolbar button.
Switch Camera Views Displayed in Video Player

Cameras and device groups can be dragged and dropped from the camera list into the Video Player for viewing.

Monitor Video of Multiple Cameras (Successively)

You can use the Video Player or the Video Monitoring window to monitor video of multiple cameras successively. To monitor video using the Video Monitoring window, refer to View a Video Tour on page 81. To monitor video of multiple cameras in matrix mode, refer to Matrix View on page 114.

To monitor video of multiple cameras successively using the Video Player:

1. Follow the procedures to Launch Video (Live/Recorded) From a Camera on page 86 in the Video Player.
2. Click and drag every camera or camera group, you will want to view, into the Video Player.
3. From the View menu select Camera. A sub-menu displays. Select the desired camera view.
4. Repeat step 3 to view different cameras successively or click the Previous Camera and the Next Camera toolbar buttons.

Capture an Image

You can capture images from live and recorded video. Images are saved as “.JPG” files.

1. Follow the procedures to Launch Video (Live/Recorded) From a Camera on page 86 in the Video Player.
2. Verify one camera view is selected; the status bar for a selected camera is blue - not gray.
3. From the Options menu select Capture Image.
4. The Multimedia Capture window is displayed.
5. Click [Export]. The Save As window is displayed.
6. Enter a file name and click [Save]. If the photo is bitmapped and the crop window is used, the portion of the image within the cropped area is saved. Otherwise, the whole photo is saved.
7. Click [OK].

Create a Video Event

Video events are automatically created in Alarm Monitoring if a camera is correctly added to a video recorder, hardware is linked to the camera and an alarm-video configuration is established.

You can also manually create a video event to lock/mark video at the exact start and stop times you desired. For example, if the OnGuard system automatically creates an event for a door forced open, but you want the event to include 5
seconds after the event occurred, you can review the video and manually create an event at the desired times.

1. Follow the procedures to Launch Video (Live/Recorded) From a Camera on page 86. Verify the recorded video is playing in the Video Player.

2. If necessary use the toolbar settings and the start and stop time fields to identify the portion of video to be marked as an event.

3. From the Options menu select Create Video Event.

4. The Create Video Event dialog is displayed. Select the appropriate Event text from the drop-down list or enter new text to append to the User Generated Video Event alarm.

5. Click [OK].

6. The Alarm Monitoring window displays a User Generated Video Event alarm.

**Matrix View**

Matrix view allows the user to view multiple video streams at once in the Video Player window. Video streams can be arranged for viewing in the Video Player using pre-configured templates. Once video streams have been added to a template, this layout can be saved so that it can be loaded by another user or monitoring station.

**Select Template Dialog**

The Select Template dialog is used to load an empty matrix view into the Video Player. Each template has a fixed number of video cells arranged in a different layout. Once a template has been loaded, drag and drop cameras from the System Status Tree to monitor them in the Video Player. The Select Template dialog is displayed by selecting View > Template from the Video Player menu.
Save Layout Dialog

The Save Layout dialog is used to create a layout that can be reused at another time. Layouts can be made available to all users or it can be limited to the current user or local workstation. The Save Layout dialog is displayed by selecting Play > Save Layout from the Video Player menu.

Save Layout Dialog

<table>
<thead>
<tr>
<th>Field(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save as new layout</td>
<td>Select this radio button to create a new layout.</td>
</tr>
<tr>
<td>Private (assigned to the current user)</td>
<td>Select this check box to make the new layout available only to the current user.</td>
</tr>
<tr>
<td>Local (assigned to this workstation)</td>
<td>Select this check box to make the new layout available only on the local workstation.</td>
</tr>
<tr>
<td>Overwrite existing layout</td>
<td>Select this radio button to replace an existing layout.</td>
</tr>
<tr>
<td>Listing window</td>
<td>Select the layout you wish to overwrite from the listing window.</td>
</tr>
<tr>
<td>Remove</td>
<td>Click this button to remove the layout selected in the listing window.</td>
</tr>
</tbody>
</table>
Load Layout Dialog

The Load Layout dialog is used to display layouts that have been previously saved by a user in the Video Player. The Load Layout dialog is displayed by selecting Play > Load Layout from the Video Player menu.

Save Layout Dialog

<table>
<thead>
<tr>
<th>Field(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private (assigned to the current user)</td>
<td>Filter the list of available layouts to display only private layouts assigned to the current user.</td>
</tr>
<tr>
<td>Local (assigned to this workstation)</td>
<td>Filter the list of available layouts to display only locally created layouts.</td>
</tr>
<tr>
<td>Listing window</td>
<td>The list of available layouts.</td>
</tr>
</tbody>
</table>

Window Size Configuration

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 PlayerWidth and PlayerHeight, <n>, represents the number of video streams. The PlayerWidth<n> and PlayerHeight<n> values should then be set to a multiple of the resolution depending on the number of cameras you want to have in each row and column. For example:

To calculate the values needed to display 8 video streams with a base resolution of 176x120 with two cameras on each of four rows, multiply the width by two cameras (176*2) and multiply the height by four rows (120*4). The following lines would need to be added to the ACS.INI file:

PlayerWidth8=352
PlayerHeight8=480
To calculate the values needed to display 6 video streams with a base resolution of 352x240 with three cameras on each of two rows, multiply the width by three cameras (352*3) and multiply the height by two rows (240*2). The following lines would need to be added to the ACS.INI file:

\[
\text{PlayerWidth6}=1056 \\
\text{PlayerHeight6}=480
\]

Matrix View Procedures

Monitor Video in Matrix View

The Video Player in matrix view can be used to view live or recorded video from multiple cameras simultaneously.

1. Follow the procedures to Launch Video (Live/Recorded) From a Camera on page 86 in the Video Player.
2. The Video Player displays. From the View menu, select As Matrix. You can also select the Matrix View toolbar button.

Note: Matrix view displays up to 32 cameras. There may be more cameras available than can fit in the viewable area. You may scroll or resize the window to view additional cameras. To resize the window hover the pointer over the corner or edge of the window until a double-headed arrow displays. Then drag the window to its desired size.

3. The screen below displays Matrix view.

Note: When viewing multiple cameras simultaneously, please note that the system automatically displays each window in such a way that it is active (the status
bar for each window is blue.) Therefore any command will be applied to every window. To deselect a window, place the cursor in the window and click. The status bar is gray when the window is deselected.

Note: For PTZ cameras in matrix mode, double clicking on a single video launches a new single video window with PTZ enabled automatically.

Create a Matrix Layout

Layouts can be configured to display video channels in a matrix view. There are multiple templates for creating layouts. Once configured, layouts can be saved and loaded on client workstations.

1. Follow the procedures to Launch Video (Live/Recorded) From a Camera on page 86 in the Video Player.

   Toolbar Shortcut

   2. The Video Player displays. From the View menu, select Template.

   3. Choose a static template from the Select Template dialog.

   4. Empty video cells are displayed in the chosen template. Click and drag cameras to the template to assign them to a video cell.

Note: Cameras can be cleared from the template by selecting them and clicking the Remove button . Selected video cells are indicated by a blue bar at the bottom the video cell, while unselected video cells display a gray bar. Video cells can be selected or deselected with a single right-click.

Save a Matrix Layout

Once cameras have been assigned to the video cells of a template, the layout can be saved for reuse by a different operator or monitoring station.

1. Follow the procedures to Launch Video (Live/Recorded) From a Camera on page 86 in the Video Player.

2. The Video Player displays. From the Play menu, select Save Layout.

3. The Save Layout dialog is displayed.

   • To create a new layout:
     a. Select the Save as new layout radio button.
     b. Enter a descriptive name for the layout.
     c. Select the Private or Local check boxes if the layout should be available only to the current user or workstation.

   • To replace a previously saved layout:
     a. Select the Overwrite existing layout radio button.
     b. Highlight the layout you wish to overwrite.
4. Click [OK] to save the layout.

**Load a Matrix Layout**

Previously saved layouts can be used by different users on different workstations.

1. Follow the procedures to Launch Video (Live/Recorded) From a Camera on page 86 in the Video Player.
2. The Video Player displays. From the **Play** menu, select **Load Layout**.
3. The Load Layout dialog is displayed. The list of available layouts can be filtered by selecting the **Private (assigned to the current user)** or **Local (assigned to this workstation)** check boxes.
4. Select a layout from the list.
5. Click [OK] to load the layout.

**Pan, Tilt, and Zoom**

Pan, Tilt and Zoom (PTZ) control is supported by all Lenel video recorders. Using PTZ you can control a camera’s movements and its ability to view images at different ranges (zoom in or out).

Digital PTZ is provided for cameras that do not have PTZ support. Digital PTZ allows the user to pan, tilt, and zoom throughout the camera’s field of view without moving the camera.

PTZ presets are imported from NetDVMS recorders when the PTZ camera channels are imported using System Administration. PTZ presets will have the same name that is configured on the NetDVMS and will be read-only in the OnGuard software. Imported NetDVMS PTZ presets are available from the Video Player.

**Configure PTZ with LNVR or LNVS Machines**

LNVR and LNVS machines do not need a matrix switcher for PTZ control. Therefore, these machines do not require special procedures in OnGuard for PTZ control; simply configure the recorder and camera.

**Configure PTZ with all other Digital Video Recorders**

LDVR, Loronix, and Generic Video machines require a matrix switcher (either real or virtual) for PTZ control. Complete the following in OnGuard to configure PTZ control for these machines.

1. Verify the default matrix switcher type settings in OnGuard are appropriate. For more information, refer to “Modify a Matrix Switcher Type” in the Matrix Switcher Folder chapter in the Digital Video Software User Guide.
2. Add the matrix switcher. For more information, refer to the Matrix Switcher Folder chapter in the Digital Video Software User Guide.
3. Configure the video recorder. For more information, refer to the Digital Video Folder chapter in the Digital Video Software User Guide.

4. Configure the camera. This includes linking the camera to the matrix switcher. For more information, refer to the Configure LDVR, Generic Video, or Loronix Cameras section of the Digital Video Folder chapter in the Digital Video Software User Guide.

Using PTZ in the Video Player

The following screen shows the addition of PTZ control in the Video Player.

- **Using the PTZ Toolbar.** Click to activate PTZ. Use the remaining buttons to pan or tilt the camera, as well as, zoom in, zoom out, and focus the camera. You can also press and hold the zoom, focus, or iris buttons to achieve the preferred view.

- **Using the Mouse.** After you click to activate PTZ you can pan, tilt, and zoom by right or left clicking your mouse in the video window. A left click moves the camera toward the cursor. The camera keeps moving in that direction until the mouse button is released. The camera moves with direction and speed determined by the mouse position relative to the center of the video window. If you move the mouse while holding the left button down, the camera changes the direction and speed accordingly. If you right-click in the top half of the screen the camera zooms in until you release the mouse. If you right-click in the bottom half of the screen the camera zooms...
out until you release the mouse. You can also use the mouse scroll wheel to zoom in/out. Scroll up to zoom in and scroll down to zoom out. The farther away from the center the mouse is the faster the camera moves.

- **Using the Keyboard.** After you click to activate PTZ you can use the keyboard arrow keys to pan, tilt, and zoom. The left and right arrow keys pan the camera left and right. The up and down arrow keys tilt the camera up and down. Hold the <Shift> key down while pressing the up or down arrows zooms the camera in or out. They keyboard keypad may also be used to control PTZ.

- **Using a Joystick.** After you click to activate PTZ you can use video controllers, such as joysticks, to pan, tilt, and zoom. Iris and focus are also available if supported by the joystick.

---

**Notes:**

The Zoom, Focus, and Iris control buttons are only enabled if the corresponding operations are supported by the camera in the current PTZ mode.

The speed of the pan and tilt operation is calculated based on the distance from the mouse click position to the center of the image along with the current zoom position. If the camera is zoomed in, the same mouse click will cause a slower movement. This functionality is subject to individual cameras. If a camera doesn’t support getting the current zoom position, the movement will not slow.

---

**PTZ Options Dialog**

The PTZ Options dialog is used to configure PTZ locking options and PTZ control behavior. PTZ controls can be customized to send either relative, continuous, or mixed commands with a single mouse click. The PTZ Options dialog is available from the **Options** menu in Alarm Monitoring.
The video window must be re-opened to use the new settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default access mode</td>
<td>Used to specify the locking mode used by default when video is launched for a PTZ camera.</td>
</tr>
<tr>
<td></td>
<td>“Locked” access mode gives control of the PTZ functions to the first user to activate PTZ. If another user attempts to activate PTZ for the same camera, they will receive a message that PTZ control is locked by another user.</td>
</tr>
<tr>
<td></td>
<td>“Shared” access mode allows multiple users to have access to the PTZ controls at the same time.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>If the Timeout (in seconds) check box is selected, you may specify an amount of time (in seconds) after which the PTZ controls will become unlocked. After this period another user may gain control of the camera.</td>
</tr>
<tr>
<td></td>
<td>For no timeout on locking, simply clear the Timeout (in seconds) check box. Unlocking will only occur when the video window is closed, PTZ control is cancelled (by deselecting the PTZ button), or PTZ locking mode is changed to shared (by deselecting the PTZ locked button).</td>
</tr>
<tr>
<td></td>
<td>Note: The PTZ timeout value is not utilized with background PTZ tours.</td>
</tr>
</tbody>
</table>
PTZ Control Adjustment Parameters

Server and client (digital) modes can be configured with different settings. Adjustments to the client modes can be only be configured by editing the ACS.INI file on the Alarm Monitoring workstation. Parameters should be placed in the [DigitalVideo] section.

Note: The video window must be re-opened to use the new settings.
### Pan and Tilt Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerMouseMode</td>
<td>Pan and tilt operations in server mode:</td>
<td>0</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td></td>
<td>• 0 = Click-to-center, then continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Drag or double-click-to-center</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: This parameter</td>
<td>This parameter can also be configured with the Mouse mode drop-down list on</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the PTZ Options dialog.</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ClientMouseMode</td>
<td>Pan and tilt operations in client (digital) mode:</td>
<td>0</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td></td>
<td>• 0 = Click-to-center, then continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Drag or double-click-to-center</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MixedPanAndTiltTimeOutMS</td>
<td>Sets the timeout value used in Click-to-center, then continuous (in milliseconds).</td>
<td>300</td>
<td>0 - 65535</td>
</tr>
</tbody>
</table>

### Zoom Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerZoomMode</td>
<td>Zoom operation in server mode:</td>
<td>0</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td></td>
<td>• 0 = Step, then continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Step mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: This parameter</td>
<td>This parameter can also be configured with the Zoom mode drop-down list on</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the PTZ Options dialog.</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ClientZoomMode</td>
<td>Zoom operation in client (digital) mode:</td>
<td>0</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td></td>
<td>• 0 = Step, then continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Step mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RelativeZoomStep</td>
<td>The number that the current focal length is multiplied (or divided) by</td>
<td>2</td>
<td>&gt;1.0</td>
</tr>
<tr>
<td></td>
<td>when the zoom in or zoom out button is pressed in step mode.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MixedZoomTimeOutMS</td>
<td>Sets the timeout value used in Step, then continuous mode (in milliseconds).</td>
<td>300</td>
<td>0 - 65535</td>
</tr>
</tbody>
</table>
### Focus Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerFocusMode</td>
<td>Focus operation in server mode:</td>
<td>0</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td></td>
<td>• 0 = Step, then continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Step mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>This parameter can also be configured with the Focus mode drop-down list</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the PTZ Options dialog.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClientFocusMode</td>
<td>Focus operation in client (digital) mode:</td>
<td>0</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td></td>
<td>• 0 = Step, then continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Step mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RelativeFocusStep</td>
<td>Determines the size of each step in step mode. Value is</td>
<td>2</td>
<td>1 - 100</td>
</tr>
<tr>
<td></td>
<td>normalized for the range of focus available for the camera.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>This parameter can also be configured with the Focus step (1-100) field</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the PTZ Options dialog.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MixedFocusTimeOutMS</td>
<td>Sets the timeout value used in Step, then continuous mode (in milliseconds).</td>
<td>300</td>
<td>0 - 65535</td>
</tr>
</tbody>
</table>

### Iris Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerIrisMode</td>
<td>Iris operation in server mode:</td>
<td>0</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td></td>
<td>• 0 = Step, then continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Step mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>This parameter can also be configured with the Iris mode drop-down list</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the PTZ Options dialog.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClientIrisMode</td>
<td>Iris operation in client (digital) mode:</td>
<td>0</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td></td>
<td>• 0 = Step, then continuous</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Step mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Continuous</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Iris Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>RelativeIrisStep</td>
<td>Determines the size of each step in step mode. Value is normalized for the range of iris available for the camera.</td>
<td>2</td>
<td>1 - 100</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This parameter can also be configured with the Iris step (1-100) field on the PTZ Options dialog.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MixedIrisTimeoutMS</td>
<td>Sets the timeout value used in Step, then continuous mode (in milliseconds).</td>
<td>300</td>
<td>0 - 65535</td>
</tr>
</tbody>
</table>

PTZ Joystick Selection

If multiple joysticks are connected to the same workstation, the ACS.INI file can be used to specify which joystick will be used. Each connected joystick is listed as a parameter in the [DigitalVideo] section as InputDeviceName1, InputDeviceName2, etc. Set InputDeviceName (without a number) equal to the joystick name you wish to use as it is written in the file.

Configure PTZ Locking

PTZ options can be configured in Alarm Monitoring.

1. From the Options menu select PTZ Options.
2. The PTZ Options dialog is displayed.
3. The Default access mode drop-down list is used to specify the locking mode used by default when video is launched for a PTZ camera.
   - Locked access mode gives control of the PTZ functions to the first user to activate PTZ. If another user attempts to activate PTZ for the same camera, they will receive a message that PTZ control is locked by another user.
   - Shared access mode allows multiple users to have access to the PTZ controls at the same time.
4. A timeout can be enabled for PTZ control with the Timeout (in seconds) check box.
   - If selected, you may specify an amount of time (in seconds) after which the PTZ controls will become unlocked. After this period another user may gain control of the camera.
   - For no timeout on locking, simply clear the Timeout (in seconds) check box. Unlocking will only occur when the video window is closed, PTZ control is cancelled (by deselecting the PTZ button), or PTZ locking mode is changed to shared (by deselecting the PTZ locked button).

Presets

Client side presets can be absolute camera positions or PTZ commands. Presets are added to the PTZ Presets drop-down and can be selected by the user to
control the camera. To open the PTZ Presets dialog, click \[\text{PTZ Monitor}^\text{TM}\] in the Video Player window to activate PTZ, then select the Options > Presets menu item or click the Preset button \[\text{PTZ Monitor}^\text{TM}\] in the PTZ toolbar.

**PTZ Preset dialog in Advanced mode**

The PTZ Preset dialog has both a simple and an advanced mode. The simple mode can be used to configure a preset for an absolute camera position or to delete an existing preset. The advanced mode can be used to configure a preset for an absolute camera position or to configure a PTZ command.

**Note:** PTZ presets that have been imported from a NetDVMS do not appear in the Type new name or select existing preset drop-down because they are not editable from the OnGuard software.

<table>
<thead>
<tr>
<th>Field</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type new name or select existing preset</td>
<td>Enter descriptive name for the preset or select an existing preset from the drop-down.</td>
</tr>
</tbody>
</table>

**Note:** PTZ presets that have been imported from a NetDVMS do not appear in the drop-down because they are not editable from the OnGuard software.
Add an Absolute Preset

To set a client side preset for an absolute camera position using the PTZ Preset dialog in simple mode:

1. In the Video Player window, click  to activate PTZ.
2. Use the PTZ controls to move the camera to the desired position.
3. From the Options menu, select Presets or click the Preset button  in the PTZ toolbar.
4. The PTZ Preset dialog is displayed in simple mode. Enter a descriptive name for the preset or select an existing preset from the drop-down.
5. If you want to overwrite an existing preset, select the Overwrite selected preset check box.
6. Return to the video player window and adjust the camera position if desired.
7. Click [OK] to save the preset.

Add a Relative or Continuous Preset

1. In the Video Player window, click  to activate PTZ.
2. From the **Options** menu, select **Presets** or click the Preset button in the PTZ toolbar.

3. The PTZ Preset dialog is displayed. Enter a descriptive name for the preset or select an existing preset from the drop-down.

4. If you want to overwrite an existing preset, select the **Overwrite selected preset** check box.

5. Click [Advanced].

6. Select the **Move relatively by** or **Move continuously** radio button.

7. Return to the Video Player window and execute the desired preset command. This will automatically populate the values in the PTZ Preset dialog.

8. Return to the PTZ Preset dialog.

9. If you are configuring a continuous command, enter the **Duration (sec)** that the camera should move for.

10. Click [Test] to view the preset in the Video Player window.

11. Make adjustments to the configuration as needed, then click [Save].

### Add a Camera Side Preset

The following procedure allows you to add preset previously configured on the camera to the system and give it a descriptive name.

1. In the Video Player window, click to activate PTZ.

2. From the **Options** menu, select **Presets** or click the Preset button in the PTZ toolbar.

3. The PTZ Preset dialog is displayed. Enter a descriptive name for the preset or select an existing preset from the drop-down.

4. If you want to overwrite an existing preset, select the **Overwrite selected preset** check box.

5. Click [Advanced].

6. Select the **Camera preset** radio button and enter the number of the camera side preset in the text box.

7. Click [Test] to view the preset in the Video Player window.

8. Click [Save].

### PTZ Tours

PTZ tours can be created using absolute camera positions and PTZ commands. PTZ tours can be run manually, continuously, or scheduled to run at specific times. PTZ tours should begin with an absolute camera preset to ensure the tour is properly executed.
**PTZ Tour Dialog**

The PTZ Tour dialog allows you to add, modify, delete, and run PTZ tours. To open the PTZ Tour dialog, click in the Video Player window to activate PTZ, then select the **Option > Tours** menu item.

<table>
<thead>
<tr>
<th>Field</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type new name or select existing tour</td>
<td>Enter descriptive name for the tour or select an existing tour from the drop-down.</td>
</tr>
<tr>
<td>Overwrite selected tour</td>
<td>Select this check box to replace an existing tour with a new configuration.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click this button to delete the selected tour.</td>
</tr>
<tr>
<td>Listing window</td>
<td>The list of the presets that make up the tour.</td>
</tr>
<tr>
<td></td>
<td>Edit the <strong>Delay (sec)</strong> column to change the number of seconds the tour should pause after executing the currently selected preset. The values allowed are 4 to 9999.</td>
</tr>
<tr>
<td>Continuously</td>
<td>Select this check box to run the tour continuously.</td>
</tr>
</tbody>
</table>
Add a PTZ Tour

PTZ tours are composed of a sequence of camera presets.

1. In the Video Player window, click to activate PTZ.

2. Use the PTZ controls in the Video Player window to move the camera to the desired start point.

3. Open the PTZ Presets dialog by selecting Options > Presets from the Video Player menu.

4. In the PTZ Preset dialog, click [Advanced].

5. Click [Current] to update the absolute position values to the current camera position.

6. Enter a name for the starting point of the tour and click [Save].

7. Open the PTZ Tour dialog by selecting Options > Tours from the Video Player menu.

8. Click <Click here to add new step> in the listing window.

9. Select the preset from the drop-down and enter the amount of time the tour should pause before the next step in the Delay (sec) column.

10. Create the next preset:

   a. In the PTZ Preset dialog, enter a preset name for the next step of the tour.

   b. Select the radio button for the type of preset you wish to configure.

   c. Return to the Video Player window and execute the command for the preset.

   d. Click [Save] in the PTZ Preset dialog.

11. Add the preset to the tour:


<table>
<thead>
<tr>
<th>Field</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the background PTZ tour server</td>
<td>Select this check box if you wish to continue running the tour after the video player has been closed. Select the PTZ tour server from the drop-down.</td>
</tr>
<tr>
<td>Note:</td>
<td>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.</td>
</tr>
<tr>
<td>Note:</td>
<td>A PTZ Tour Server must be configured on the Digital Video &gt; PTZ Tour Server tab in System Administration to run a tour continuously in the background.</td>
</tr>
<tr>
<td>Save</td>
<td>Click this button to save the tour.</td>
</tr>
<tr>
<td>Exit</td>
<td>Click to exit the PTZ Tour dialog.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>Use the [Up] and [Down] buttons to reorder the presets in the listing window.</td>
</tr>
<tr>
<td>Remove</td>
<td>Remove the selected step from the tour.</td>
</tr>
<tr>
<td>Run</td>
<td>Click this button to test the tour in the video player window.</td>
</tr>
</tbody>
</table>
a. In the PTZ Tour dialog, click `<Click here to add new step>` in the listing window.
b. Select the preset from the drop-down.
c. In the **Delay (sec)** column, enter the amount of time the tour should pause before executing the next step of the tour.

12. Repeat steps 10 and 11 to add additional steps to the tour.

13. When you have finished creating the tour, click [Save] in the PTZ Tour dialog.

### Run a PTZ Tour

1. In the Video Player window, click ![ PTZ button ] to activate PTZ.
2. Launch the PTZ Tour dialog by selecting **Options > Tours** from the Video Player menu.
3. Select the PTZ tour from the listing window drop-down.
4. Click [Run].

**Note:** The Preset button in the PTZ toolbar will remain pressed while the tour is running. To interrupt the tour, simply execute any PTZ command or menu option. The tour will also stop if control is taken over by another user with higher PTZ priority level or when the PTZ control is given up by closing the video window or deselecting the PTZ button. If the tour is set to run in the background, an option will be given to resume the tour once PTZ control is relinquished.
Video verification is the process of comparing “live” (as it is happening) video with a photograph stored in the database. When a person swipes a badge through a reader, you can use video verification to compare the cardholder’s photo.

The Video Verification window can be displayed several ways:

- Select the Video Verification toolbar button.

  **Toolbar shortcut**

- From the View menu select Video Verification.
Video Verification Configuration Dialog

Video verification type
Select Use digital video verification if you are using cameras that connect to a video recorder or Use standard video verification if you are using CCTV.

Use all video enabled readers
Select this check box to use all readers that have a Device-Camera Link established in System Administration.

Reader listing window
If you do not wish to use all applicable readers, select each camera that you wish to use individually.

Maximum number of videos to display
Select a number 1-10 from the drop-down list to indicate the maximum number of items you wish to display in the Video Verification window.

Digital Video Verification
Digital Video Verification is used with cameras connected to a video recorder.

- Live video and cardholder information is displayed for each video verification item.
- Multiple video verification views can be displayed concurrently in the Digital Video Verification window. The most recent view appears on top.
- If multiple cameras are linked to a device, the camera with the View Order of 1 (from the Device-Camera Links form in System Administration) will be displayed.
Set Up Digital Video Verification

Several procedures must be completed in System Administration prior to using Digital Video Verification. Refer to the System Administration User Guide for additional information about each of the following steps.

1. Configure the video recorders and cameras that will be used with Digital Video Verification.
2. Configure the additional devices (such as readers) that will be used with the cameras for video verification.
3. Configure a Device-Camera link for each camera and device pair. If more than one camera is associated with a device, the camera with a view order of 1 is used with video verification.

Standard Video Verification

Standard Video Verification is used with CCTV cameras.

- Alarms are displayed in the Video Verification window.
Video Verification

Standard Video Verification Window

Panels/readers window
Lists all panels and readers in the system.

Selected readers
Contains those readers from which the Video Verification window will receive information. If this list is empty, no alarms will display in the Video Verification window.

Live video
Displays live video from a CCTV (camera) device at a specific location.

If you see a black box instead of live video, it means that either there is no camera available or the camera isn’t working properly.

If you see a “Live video not available” message, it means that your System Administrator has made live video from that location unavailable to Alarm Monitoring stations.

Photograph
Displays a specific cardholder record photo.

On new event display
Includes the Photograph and Video check box fields.

- Video: If checked, pan, tilt and zoom CCTV commands are automatically enabled. If unchecked, pan, tilt and zoom CCTV commands must be manually invoked. Live video remains visible regardless of the state of this check box.

- Photograph: If checked, as each new alarm arrives, the corresponding cardholder photo displays.

Alarms window
Lists alarms as they arrive. Each row represents one alarm. Click the following column headings to arrange alarms by that heading:

- Alarm Description: Name of the alarm
- Cardholder: Cardholder’s name and Badge ID
Standard Video Verification Procedures

Use the following procedures for standard video verification.

Add or Remove Readers

To add or remove readers using the video verification window, the reader must be added to the Selected Readers list.

Note: The Panels/Reader list is located in the upper left portion of the Video Verification window. The Selected Readers list is located in the lower left portion of the Video Verification window.

- To add an entry to the Selected Readers list, double-click the reader in the Panels/Readers list.
- To add a new entry to the Selected Readers list, select one or more alarm(s) before you open the Video Verification window, the corresponding reader(s) will be added automatically.
- To add all the readers associated with a particular panel, double-click the panel entry in the Panels/Readers list.
- To remove a reader from the Selected Readers list, double-click the reader’s entry in the Selected Readers list.

Display the Cardholder Photo and Live Video

Clicking an alarm in the video verification alarms window displays both the cardholder photo and live video from a camera at the reader. Live video continues to display until one of the following happens:

- You click another alarm.
- Another alarm arrives (this is true only if the Video check box is selected.)

Notes: The Video check box must be selected to display live video when a new alarm occurs. The Photograph check box must be selected to display the cardholder’s photograph when a new alarm occurs.

Delete an Alarm in the Video Verification Window

- To remove an alarm from the alarms window, click the alarm then select Delete from the Edit menu or right-click the alarm and select Delete.
- To clear all alarms from the alarms window, select Delete All from the Edit menu.
Cardholder verification is the process of viewing a cardholder’s photo “live” (as the cardholder is badging through a reader). When a cardholder swipes a badge through a reader, that user’s photo is displayed in the Cardholder Verification Configuration window. You can use cardholder verification to compare the cardholder’s photo to that of the person using the reader.

The Cardholder Verification window can be displayed by clicking View > Cardholder Verification.

If the Cardholder Verification window is open when the Alarm Monitoring application is closed then the Cardholder Verification window will open automatically next time the application is launched.
Cardholder Verification Window

Reader drop-down box
Choose a reader from this drop-down box to view the cardholder images from the badge being used.

Set up Cardholder Verification
1. In Alarm Monitoring, click View > Cardholder Verification. The Cardholder Verification window opens.
2. In the drop-down box, select the reader whose cardholders you would like to view.
3. As the cardholder badges through the selected reader their photo will appear in the Cardholder Verification window.
4. Repeat steps 1-3 to open multiple Cardholder Verification windows to cover multiple readers at once.
Permissions for control device groups can be given or restricted through System Administration. From the Administration menu select Users. On the Monitor Permission Groups sub-tab there is a Control Device Groups sub-tab with which you can control access to device groups.

Grant/Deny Pop-up Window

Your System Administrator can configure any input event for any device to execute an output action that launches a grant/deny pop-up window associated with a door/reader. Alarm Monitoring operators with the correct permissions can either grant or deny access through the door/reader. When a grant is issued the door is pulsed open. When a deny is issued, no command is sent.

Note: For configuration procedures refer to the Global I/O Folder chapter in the System Administration User Guide.

Alarm Monitoring stations and operators monitoring the same zone the input device/event and output device/event are configured for are notified when the input event occurs.

Display area
Displays any and all active requests. The display window contains the following columns:

- Destination Device - The door/reader the output action will affect.
- Initiating Device - The device the request is coming from.
Both the initiating device and destination device must be in the same monitor zone.

- Alarm - The input event that is linked to an output action.
- Alarm Time - The time the request was initiated.
- Timeout - The total amount of time the operator has to either grant or deny the request. The timeout value is user-defined with a default value of 3 minutes. This field does not refresh. To determine the amount of time remaining the operator must also refer to the Alarm Time column. The current time located in the status bar determines when the request was initiated.

**Grant**

Grants the request (pulses open the door) and removes the request from the Grant / Deny pop-up window.

**Deny**

Denies the request (no command is issued to the hardware) and removes the request from the Grant/Deny pop-up window.

**Grant/Deny Pop-up Window Procedures**

Use the following procedures in this window.

**Grant or Deny Access**

1. Verify the Communication and Linkage Server are running. To do this, click the Start button then select *Programs > OnGuard 2013 > Service and Support > Communication Server or Linkage Server*.

2. To grant access, complete one of the following when the Grant/Deny pop-up window displays:
   - Double-click a request.
   - Right-click a request and select Grant.
   - Select (highlight) a request and click [Grant].

    **Note:** You must have the open door user permission in order to issue a grant. Contact your System Administrator to set up this permission or refer to the Users Folder chapter in the System Administration User Guide for procedures.

3. To deny access, complete one of the following when the Grant/Deny pop-up window displays:
   - Let the timeout value expire by doing nothing.
   - Right-click a request and select Deny.
   - Select (highlight) a request and click [Deny].

    **Note:** A user transaction is logged when a grant or deny occurs.

**Right-click Options to Control Devices and Areas**

You can control devices and areas through a wide variety of right-click and left-click menu options available in Alarm Monitoring. You can right-click and left-click icons in map view, right-click alarms, right-click device groups as well as right-click and left-click hardware in the System Status.
Right-click Options to Control Devices and Areas

window. The menu options available when you right-click or left-click depend on the window you are in and the device or area you are clicking on.

Some right-click and left-click menus contain sub-menus. To execute commands you must first select the device from the right-click or left-click menu. A sub-menu of options displays to control that device.

Note: Many of the right-click and left-click options are also available as options from the main menu.

General Right-click Options
These right-click options can be available for alarms as well as multiple devices/hardware.

- Acknowledge - acknowledges the currently selected alarm.
- Trace - traces the selected device.
- Update Hardware Status - polls currently selected access panel/controller and updates the hardware status. If a downstream device (like a reader) is selected, the update hardware status is done for the controller associated with that device.
- View Map - displays a map associated with the selected device (if one exists). If more than one map exists, the user is prompted to select a map.
- Launch Video - displays video for the selected device if a camera is associated with the device.

Monitor Zone Right-click Options
- Update All Hardware Status - updates the display to show the currently status of all devices.
- Set All Controller Clocks - sets all clocks to the current system time.
- Trace Monitor Zone - traces a monitor zone.

Access Panel and Alarm Panel Right-click Options
- Properties - available for access and intrusion panels.
- Open Door(s) - opens the door(s) associated with the selected access panel. If using Recognition Source readers this option will not be available, because these specific readers are not in constant communication with the PIM devices.
- Set Controller Clock - sets selected access panel/controller clock to current time. If a device other than an access panel/controller is selected, this option sets the clock on the access panel/controller to which the device is attached.
- Reader Access Modes - updates the reader mode of every reader associated with selected access panel/controller or reader.
  - Card and Pin: Sets the reader to card and pin mode.
  - Card Only: Sets the reader to card only mode.
  - Pin or Card: Sets the reader to pin or card mode.
  - Cipher Lock Emulation: Sets the reader to cipher mode requiring a master combination or “cipher code”.
  - Facility Code Only: Sets the reader to facility code only mode.
  - Locked: Locks the reader.
  - Unlocked: Unlocks the reader.
  - Default: Sets the reader to the default online mode that it is configured for in the database.
Control Devices and Areas

- Lock Door - NGP only. Select to lock both the in and out reader.
- Unlock Door - NGP only. Select to unlock both the in and out reader.
- Reinstate Door - NGP only. Select to put both the in and out reader into a locked state until the proper credentials are presented putting the reader into the last known access mode.
- Reader Verify Mode - used to enable or disable verify mode for access control readers with an associated secondary reader. When verify mode is enabled, access to both the primary and secondary reader is required. When verify mode is disabled, only access to the primary reader is required.
- Activate - activates the outputs associated with the selected access panel.
- Deactivate - deactivates the outputs associated with the selected access panel.
- Pulse - pulses all outputs associated with the selected access panel.
- Mask - masks inputs or alarms for the currently selected reader.
- UnMask - unmasks inputs or alarms for the currently selected reader.
- Download Firmware - downloads firmware to the selected controller, LNL-1100 or LNL-1200 alarm panel or RS-485 command keypads. Controllers and gateways display firmware revision numbers using three decimal places, while downstream devices display the firmware revision number using two.

1200 (Firmware Revision: 1.04)

- Download Database - downloads the database to the access panel/controller.
- Download Encryption Keys - downloads the encryption keys to the panel and from the panel to any connected devices over an RS-485 connection. Encryption keys can only be transferred over an encrypted connection. This option is available for LNL-3300 and LNL-2220 panels only.
- Reset Use Limit - resets the number of times a badge can be used on a particular access panel/ controller.
- Connect - connects the access panel/controller via a dialup/modem connection.
- Disconnect - disconnects the access panel/controller via a dialup/modem connection.

Intrusion Area Right-click Options

- Disarm (all intrusion controllers) - Disarms the area.
- Perimeter Arm (Detection Systems only) - Arms the perimeter of an area.
- Arm Entire Partition (Galaxy and Detection Systems only) - Arms the perimeter and interior points of an area.
- Partial Arm (Galaxy only) - Arms only the zones marked for partial set in the controller.
- Master Arm Delay (Bosch only) - Arms the perimeter and interior points with exit and entry delays.
- Master Arm Instant (Bosch only) - Instantly arms both the perimeter and interior points.
- Perimeter Delay Arm (Bosch only) - Arms the perimeter with exit and entry delays.
- Perimeter Instant Arm (Bosch only) - Instantly arms the perimeter points.

Intrusion Panel Right-click Options

In addition to the acknowledge, trace, update hardware status, properties and set controller clock right-click options, intrusion panels and relays can also have the following right-click option.

- Execute Custom Function - executes a custom function associated with the Bosch Intrusion Controller. This menu option is only available with Bosch Intrusion Controllers.
Intercom Right-click Options

- Place Call - displays a dialog box where you enter the station number you are calling to.
- Call Intercom - places a call using the intercom station configured in System Administration > Monitoring > Monitor Zones, and then selecting the Monitor Stations tab.

**Note:** Calls made using the Call Intercom function are always assigned Low Priority or Priority 0.

- Cancel Call - cancels the intercom call.
- Badge Information - displays badge information associated with the intercom event; who placed the call and/or who received the call. If an intercom event has two intercom stations associated with it (the station that placed the call and the station that received the call) a dialog displays, allowing alarm monitoring operators to select the intercom station(s) they want to base the cardholder search on.

**Note:** The Badge Information right-click option is only available for intercom stations linked with the customized cardholder field, Cell number. For more information, refer to the Cardholder Options folder - Automatic Lookup form in System Administration.

Ericsson MD110 Intercom Right-click Options

**Note:** The Ericsson MD110 allows calls to be queued. If a call is queued, a Call Queued alarm is sent to Alarm Monitoring.

- Place Call - displays a dialog box where you enter the station number you are calling to.
- Cancel Call - cancels the intercom call.
- Cancel all Calls - cancels all calls.
- Block Station - blocks the station from receiving a call.
- Unblock Station - lets the station receive calls again.
- Divert This Call - for a call that has been queued. Displays a dialog box that allows you to divert the call to another station. That station will then receive a ringing alarm, which you then handle as normal.

Intrusion Door Right-click Options

Bosch is the only intrusion controller that supports doors.

- Open Door - Opens the door for the selected intrusion panel.
- Door Mode - Changes the current door mode.
  - Lock - Locks a door and requires a proper user ID to allow access.
  - Unlock - Unlocks the door allowing free access to everyone.
  - Secure - Locks the door prohibiting access for anyone.

Intrusion Relay Right-click Options

The information in this section applies to both onboard and offboard relays except where noted otherwise.

- Activate - Activates the outputs associated with the selected intrusion panel.
- Deactivate - Deactivates the outputs associated with the selected intrusion panel.
• Toggle - Puts the output in the opposite state of the current state. For example, if the output is currently set to activate then this command will set the output to deactivate. This command is available for Bosch Offboard relays only.

**Intrusion Zone Right-click Options**

- Bypass - Masks the zone from reporting alarm or tamper activity.
- Unbypass - Unmasks the zone so that any tamper or alarm activity for the zone will be reported.

**Reader Right-click Options**

In addition to several options listed in Access Panels and Alarm Panels, right-click options for readers also include:

- Download Reader Firmware - downloads firmware to the selected dual interface Rdr1 reader. Displays the major and minor firmware revision number. The minor firmware revision number displays as the last two digits.
- Reader Biometric Verify Mode - enables/disables verify mode for access control readers with an associated biometric reader. When verify mode is enabled, the normal card and/or pin access and a biometric match is required. When verify mode is disabled, only the card and/or pin access is required.
- Reader First Card Unlock Mode - enables/disables the Reader First Card Unlock Mode. The Reader First Card Unlock Mode is a qualifier for online Reader Mode. When enabled, the online Reader Mode is in effect until the first (qualified) access granted with entry occurs. When the first access granted with entry occurs, the online Reader Mode changes to unlocked.

**Note:** Reader First Card Unlock Mode is only supported on the LNL-2000 controller. However, first style unlock behavior can be configured for use with any access controller through Lenel’s Global I/O Support.

**Reader Group Right-click Options**

- Secure All - locks all doors in the reader device group and sets all readers to the locked mode.
- Unsecure All - unlocks all doors in the reader device group that were previously secured, and sets all readers to the unlocked mode.
- Reader Access Modes - sets all readers in a reader device group to a specified reader access mode.

**Note:** Only reader access modes which are supported by the entire group will be available.

For example, Unlocked and Card Only will be the available modes for the following group of readers:

- Reader 1 (Unlocked, Card Only, Secured, Unsecured)
- Reader 2 (Unlocked, Card Only, Card and Pin, First Card Unlock)
- Reader 3 (Unlocked, Card Only, Secured, Unsecured)

**Alarm Mask Group Right-click Options**

- Group Mask - masks inputs or alarms for the currently selected reader.
- Group Unmask - unmasks inputs or alarms for the currently selected reader.
Intrusion Mask Group Right-click Options

- **Disarm/Reset** - Disarms the Intrusion Mask Group. If the intrusion mask group is armed it will transition to be disarmed if no alarm is made. If the intrusion mask group was in an alarm state, it will transition into an alarm cancelled state until the same command is executed again to transition it into a disarmed state.

- **Arm Away** - Arms all points of the mask group. Any point activation will either trigger an alarm or start the entry or exit delays. Exit delays start at the time arming occurs, and allows exit through trigger points for the user set duration.

- **Arm Stay** - Arms the perimeter points of the mask group but does not arm the points defined as interior. This mode allows movement inside the protected area, but will trigger an entry delay and subsequent alarm if any perimeter point is activated. Exit delays start at the time arming occurs, and allows exit through trigger points for the user set duration.

- **Arm Stay Instant** - Arms the perimeter points of the mask group but does not arm the points defined as interior. This mode allows movement inside the protected area but will trigger an entry delay and subsequent alarm if any perimeter point is activated. There is no exit delay.

- **Restore All Points** - Removes bypass settings for all points in the intrusion mask group.

Function List Right-click Options

*Function lists* are keypad-activated commands that are programmed into an access panel. Function lists can be accessed by assigning them to specific keypad sequences.

- **Execute: True** - sets the logic term to true.
- **Execute: False** - sets the logic term to false.
- **Execute: Pulse** - temporarily sets the logic term to true.

Action Group Right-click Options

In addition to the view map option, action groups also include execute as a right-click option.

**Note:** Action groups will display if the logged in user has the segment access to the action group along with permissions to execute all of the actions in the action group.

Anti-Passback Area Right-click Options

These right-click options are unique to areas and area alarms. There are other right-click options available for areas and they are listed in General Options.

- **Update Area Status** - updates the status of both safe and hazardous areas so that operators can have a current view of cardholder locations.
- **Occupancy Report** - provides a current report of the cardholders currently in a safe area.
- **Move Badges** - enables an operator to manually move all the badges from one area to another.
- **Mustering Report** - provides a current report of the cardholders currently in a hazardous area.
- **Start Muster Mode** - initiates Muster mode. The Start Muster Mode window displays and provides an area to enter comments.
- **Reset Muster Mode** - ends Muster mode. The Reset Muster Mode window displays and provides an area to enter comments.
Guard Tour Right-click Options
These right-click options are available if Guard Tour is set up in your system.

- Launch Tour - starts a guard tour.
- View Tour - displays the guard tour live tracking window for a specific tour.

Remote Monitor Right-click options
In addition to several options listed in Access Panels and Alarm Panels, right-click options for Remote Monitors also include:

- Launch Video - launches the local monitor window in Alarm Monitoring.
- Download Database - synchronizes the RM with the camera channels assigned in Alarm Monitoring.
- Remove All - removes all video from the RM.
- Matrix - switches the RM to matrix view.
- Single - switches the RM to single player mode.
- Next - in single player mode, selects the next video cell in the list.
- Prev - in single player mode, selects the previous video cell in the list.
- Live - changes to live video on each video cell in the RM.
- Recorded - changes to recorded video on each video cell in the RM.
- Pause - pauses the video playback on each video cell.
- Play - resumes the video playback on each video cell.
- Stop - stops the video playback on each video cell.
- Frame Advance - advances one video frame on each video cell.
- Fast Forward End - fast forwards to the end on each video cell.

Remote Monitor Video Cell Right-click Options
In addition to several options listed for Remote Monitors, these right-click options are available for video cells assigned to Remote Monitors (RM):

- Launch Video - launches video on the RM and the local monitor window in Alarm Monitoring.
- Remove - removes the video cell from the RM.
- Select - in matrix view, changes to single player mode with the selected video cell.

Elevator Terminal Right-click Options
These right-click options are available if elevator dispatching is configured in your system:

- Set Allowed Floors - updates which floors and doors are accessible via the elevator terminal without supplying security credentials.
- Elevator Terminal Modes - updates the elevator terminal’s operational mode for interacting with the cardholder:
  - 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.
  - 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.
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.

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.

Single and Double Left-click Mode

Each Alarm Monitoring operator can set their options so that commands are executed with a single left-click or a double left-click of an icon in the system status view or map view. The default setting is to execute commands with a double left-click.

Furthermore, if that command was previously available as a right-click menu option, then the command will be listed in bold when the device is right-clicked. For some menus, the default command may be in a sub-menu of the context menu. The example that follows shows the Reader Auxiliary Output # 2 in bold. This is the command that will be executed when the operator single or double left-clicks the controller icon, depending on how they have set their options.

Note: Using the System Administration application your System Administrator can associate commands with a device or area icon so that when the icon is single or double left-clicked in Alarm Monitoring, the command is executed. For information on how to associate a command with a device or area icon, refer to the Monitoring Options Folder Chapter in the System Administration User Guide.

Activate Single or Double Left-click Mode

Single or double left-click mode is configurable per user. To activate single left-click mode select (place a checkmark beside) the Execute Command on Single Click of Icon in the Options menu of Alarm Monitoring. While in this mode you can single left-click an icon in the Alarm Monitoring system status and map view to execute the command configured for that device or area.
To activate double left-click mode deselect (there is no checkmark beside) the *Execute Command on Single Click of Icon* in the *Options* menu of Alarm Monitoring.

**Select a Device in Single or Double Left-click Mode**

**Single Left-click Mode**

In single left-click mode you can select a device, by placing or hovering the cursor near the device without left-clicking. The system status list and tree view identifies a selected device by underlining and/or highlighting the device.

The map view identifies a selected device by displaying the tool tip.

**Double Left-click Mode**

To select a device in double-click mode, left-click the device.

**Execute a Command in Single or Double Left-click Mode**

**Single Left-click Mode**

To execute a command in single left-click mode, left-click the device. Clicking the expand symbol in tree view does not execute the command.

**Double Left-click Mode**

To execute the command, double left-click the device.

**Note:** If you are in double left-click mode in the System Status view, not only do you execute the command when you double left-click a device, but you also expand or collapse the hardware list.
When an alarm occurs, it displays in the Main Alarm Monitoring window. Each alarm displays in its own row and is preceded by a colored dot. If alarms are configured in the System Administration software so that they do not automatically delete after they are acknowledged, an alarm icon will also display beside the colored dot after it is acknowledged.

Alarm Icons

The following table is a list of the different types of alarm icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Alarm acknowledged without notes.</td>
</tr>
<tr>
<td>🔄📝</td>
<td>Alarm acknowledged with notes.</td>
</tr>
<tr>
<td>📥️</td>
<td>Green colored dot indicates a restored alarm.</td>
</tr>
<tr>
<td>📥️</td>
<td>Two green colored dots indicate a restored alarm from a secondary channel connection.</td>
</tr>
<tr>
<td>🔄️</td>
<td>Red colored dot indicates an active alarm.</td>
</tr>
<tr>
<td>🔄️</td>
<td>Two red colored dots indicate an active alarm from a secondary channel connection.</td>
</tr>
<tr>
<td>🔄️</td>
<td>Outstanding acknowledgment action is associated with the alarm. An acknowledgment action is an action that will automatically be carried out when the alarm is acknowledged.</td>
</tr>
</tbody>
</table>
Pending Alarms Window

The Pending Alarms window is similar to the Main Alarm Monitoring window in that it has the same menu options and toolbars. However, the Pending Alarms window only displays pending alarms, which are alarms that are configured to require an operator to take action. Pending alarms are highlighted in the Main Alarm View and cause Alarm Sprites to be shown on graphical maps for the devices associated with those pending alarms.

Alarms are configured to be pending alarms in the Alarm Definitions Form in System Administration. If events configured here are set to be “active” then their corresponding alarm will be highlighted in the Main Alarm Monitoring window. For more information see the Alarm Configuration Folder chapter in System Administration.

An example of a pending alarm can be anything depending on the configuration done in System Administration. Commonly though, higher need alarms such as a door being forced open are reserved for this type of immediate action.

If the Pending Alarms Window is left open, the window automatically updates itself. For example, when a pending alarm is acknowledged in the Main Alarm Monitoring window, it immediately ceases to display in the Pending Alarms window.

If a pending alarm is an initiating alarm that becomes physically restored and must be acknowledged, it continues to display as a pending alarm until it is acknowledged. If a pending alarm is an initiating alarm that becomes physically restored but does not require acknowledgment, the alarm ceases to be a pending alarm.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Camera" /></td>
<td>Camera is associated with the device that the alarm occurred on/for. Therefore you can pull up live video via the Launch Video right-click menu option.</td>
</tr>
<tr>
<td><img src="image" alt="Alarm" /></td>
<td>Alarm acknowledged without notes and a camera is associated with the device.</td>
</tr>
<tr>
<td><img src="image" alt="Alarm" /></td>
<td>Alarm acknowledged with notes and a camera is associated with the device.</td>
</tr>
<tr>
<td><img src="image" alt="Alarm" /></td>
<td>An outstanding acknowledgment action is associated with the alarm and a camera is associated with the device.</td>
</tr>
<tr>
<td><img src="image" alt="Camera" /></td>
<td>Digital video associated with the alarm has been marked.</td>
</tr>
<tr>
<td><img src="image" alt="Alarm" /></td>
<td>Alarm acknowledged without notes and has archived video.</td>
</tr>
<tr>
<td><img src="image" alt="Alarm" /></td>
<td>Alarm acknowledged with notes and has archived video.</td>
</tr>
<tr>
<td><img src="image" alt="Camera" /></td>
<td>Outstanding acknowledgment actions and archived video.</td>
</tr>
<tr>
<td><img src="image" alt="Camera" /></td>
<td>Alarm marked in progress.</td>
</tr>
</tbody>
</table>
An initiating alarm is automatically deleted upon arrival of its corresponding canceling alarm. (e.g. Door Forced Open/Door Forced Open Canceled).

Like the Main Alarm Monitoring window, you can determine the type of information displayed about alarms through the Configure > Columns menu option. However, you cannot filter the type of alarms displayed through the Configure > Alarm Filter menu option. That is because the Pending Alarms window is intended to summarize ALL pending alarms.

**Toolbar Shortcut**

To display the window, select the Pending Alarms option from the View menu or click the View Pending Alarms toolbar button.

To view tables of the menu items and toolbar options, refer to Menus and Toolbars on page 32.

**Procedure for Monitoring Alarms**

Use the following procedures for monitoring alarms.

**Sort Alarms**

Alarms are listed in the order indicated by the sort criterion. To determine the current sort criterion locate “Sort criteria” in the status bar (lower right side of the screen).

You can rearrange the order of existing and new alarms using either of these two methods:

- Clicking a column heading
- Selecting View > Sort by from the Main Alarm Monitoring menu.

The choices available in the Sort by submenu are:

**Alarm Description**

Lists alarms alphabetically by alarm description.
Monitor Alarms

Account Group
List alarms in order of receiver account group (panels). Receiver accounts are used to represent panels in a receiver setup.

Asset Name
List alarm alphabetically by asset name.

Asset Scan ID
Lists alarms in order of asset scan ID.

Associated Text
Indicates (Yes or blank) whether there is additional text associated with the alarm.

Badge Type
Displays the badge type associated with the alarm.

Biometric Score
Lists alarms in order of biometric score. A biometric score is based on how well a biometric access control reader matches a template in the database. By default, this sort option is not enabled. To enable this sort option, the “Biometric Score” column must first be added via the Configure > Columns menu option in Alarm Monitoring.

Card
Lists alarms numerically by the card number (badge ID), if the alarm is associated with a cardholder.

Controller
Lists alarms alphabetically by name of the controller with which the alarms are associated. The controller can be an access panel, fire panel, intercom exchange, receiver or receiver account.

Controller Time
Lists alarms in order of controller time. The time includes the hour and minute and the date includes the month, day and year. The display is based on the time zone setting selected in the Control Panel of your computer. Typically the display is adapted to the country in which you are located.

Device
Lists alarms alphabetically by name of the device (reader, alarm panel, intercom station etc.) associated with the alarm. If the alarm originates at a reader, the reader name displays. If the alarm originates at an alarm panel, the panel name displays. If the alarm originates at a video recorder, the recorder name displays.

Input/Output
Lists alarms alphabetically by name of the alarm input, if the alarm is generated at an alarm input.

Intercom Station Called
Lists alarms in order of intercom station called.

Intrusion Area
Indicates the name of the area associated with the alarm. This is only displayed when the controller reported an area number along with the alarm.
**Line Number**
Displays alarms in order of line number.

**Priority**
Lists highest priority alarms at the top of the list, followed by medium priority alarms, with low priority alarms placed at the bottom of the list.

**Time/Date**
Lists alarms in chronological order. Within a given date (month, day and year) the alarms are sorted by time, which include hours and minutes and optionally seconds.

To view time in seconds go to the *Options* menu and select (place a checkmark beside) *Display Seconds*.

To view the most recent alarms at the bottom of the list, go to the *Options* menu and select (place a checkmark beside) *Ascending Time/Date*. To view the most recent alarms at the top of the list select (place a checkmark beside) *Descending Time/Date*.

**Transmitter**
Lists alarms in order of transmitter. *Transmitters* are devices that generate either an RF or IR (or both) signal that Visonic SpiderAlert receivers can receive. There are three types of transmitters: fixed, portable (hand-held) and man-down.

For more information refer to the Personal Safety Devices Folder chapter in the System Administration User Guide.

**Transmitter Input**
Lists alarms in order of transmitter input.

For any sort, the second level sort criterion is always Priority and the third level criterion is always Time/Date. For example:

- If you sort by Controller, all alarms associated with the same controller will be sorted by Priority then by Time/Date.
- If you sort by Priority, all alarms with the same priority will be sorted by Time/Date.
- If you sort by Time/Date, alarms with the same time (to the second)/date will be sorted by Priority.

The sort criterion applies to the current window only. You can have one Main Alarm Monitoring window and various Trace windows, each with a different sort criterion. When you open a new Main Alarm Monitoring window, it is initially sorted by Priority.
When you acknowledge an alarm, you provide a software response to it. Your system administrator can configure alarms so they have to or do not have to be acknowledged before they are deleted from the Main Alarm Monitoring window. Furthermore, your System Administrator can associate actions with an alarm so when the alarm is acknowledged an action or group of actions is automatically triggered.

Alarms can be acknowledged from the Main Alarm Monitoring window, the Trace Monitor window, the Pending Alarms window, or the Video Verification window.

Note: An action is any task performed by software as a result of an event or schedule.

Alarm Acknowledgment Window

The Alarm Acknowledgment window enables you to:

- Respond (in the software) to an alarm.
- View or listen to stored instructions for a specific alarm.
- Print information pertaining to an alarm.
- Enter or select notes pertaining to an alarm.

The Alarm Acknowledgment window can be displayed several ways:

- Double-click an alarm.
- Highlight an alarm entry and from the Edit menu select Acknowledge.
- Right-click an alarm entry and select Acknowledge.
Description
Contains the same name for the alarm as indicated in the Main Alarm Monitoring window.

Controller
Displays the name of the access panel/controller associated with the alarm.

Input/output
If the alarm originated at an input/output device, displays the name of the device.

Time/date
Displays the time and date the alarm occurred.

Device
If the alarm originated at a video recorder, displays the name of the video recorder. If the alarm originated at a reader, displays the name of the reader.
If the alarm originated at an alarm panel, displays the name of the alarm panel.

Card
If the alarm is card-related, displays the cardholder name (if known*) and the badge ID.
*Cardholder name would not be available for an “Invalid Badge” alarm, for example. This field is not used for OnGuard.

Original notes
Displays any notes carried forward from the associated original alarm.

Notes
Enables you to add your own comments/response to the selected alarm.

Select
Displays a window where pre-configured acknowledgment notes can be selected.

Instructions
Displays pre-configured instructions pertaining to the alarm.

Audio
Plays audio instructions.
**Alarm Acknowledgment Procedures**

Use the following procedures in this window.

**Acknowledge an Alarm**

1. Display the Alarm Acknowledgment window by double-clicking an alarm.
2. If the alarm has text instructions associated with it the information displays in the Instructions sub-window. Click [Print] to print the instructions.
3. If the alarm has voice instructions click [Audio].
4. To select pre-configured acknowledgment note(s) click [Select]. The Select Acknowledgment Notes dialog appears. Select the name of the pre-configured note and click [OK].
5. To add notes to the alarm, type your comments and click in the Notes sub-window. If this is a canceling alarm, any notes carried forward from the associated initiating alarm gets displayed in the **Original Notes** field.

**Note:** If your System Administrator has configured the alarm to be marked “in progress” before being acknowledged continue to step 6. If not, move on to step 8.

6. If you are unable to acknowledge an alarm click [In Progress]. This marks the alarm as being “in progress” and acts as a state in between an unacknowledged and acknowledged alarm.
7. One an alarm is marked “In Progress” you are able to update the notes by clicking [Update]. Each update is time stamped with the date and time.

8. Click [Acknowledge] to acknowledge the alarm.
   • If your System Administrator has configured this alarm type for “Require Login On Ack.” you must first log in before this alarm can be acknowledged.
   • If this is an initiating alarm, the corresponding canceling alarm may not be displayed until you acknowledge this alarm. Whether this happens depends upon how your system is set up.
   • Your System Administrator may have set up some types of alarms to be automatically deleted from the Main Alarm Monitoring window after you acknowledge them. If this is not the case, delete the alarm manually. For more information, refer to Delete an Alarm on page 161.

9. You can acknowledge multiple alarms without closing the Alarm Acknowledgment window. Repeat step 2 through 8 for each alarm you display in the Alarm Acknowledgment window. Use the navigation buttons to move through the list of alarms.

10. To close the Alarm Acknowledgment window, click [Close].

**Fast/Group Acknowledge Alarms**

The Fast/Group Acknowledge feature allows you to acknowledge a group of alarms simultaneously. This feature can be used without bringing up the acknowledgment dialog box.

1. Select the alarm(s) that you wish to acknowledge.
   • To choose two or more alarms, hold down the <Ctrl> key while selecting additional alarms.
   • To select all the alarms press <Ctrl> + <F11>.

2. Acknowledge the group of alarms by completing one of the following:
   • Choose Fast/Group Acknowledge from the Edit menu
   • Right-click the selected group of alarms and choose Fast/Group Acknowledge
   • Click the Fast/Group Acknowledge toolbar button

   **Toolbar Shortcut**

   • Press <Ctrl> + <F12>

3. A message displays:

4. Click [Acknowledge] to confirm the acknowledgment of the alarms.

**Notes:** If any of the chosen alarms require notes upon acknowledgment, you will be prompted to enter notes.

If any one of the alarms has already been acknowledged, it cannot be re-acknowledged. A message displays to inform you of how many alarms have been acknowledged. Click [OK] and delete the alarm(s).
The configuration for any given alarm may require that the operator log in upon acknowledging the alarm. If this is the case the user will be prompted to log in.

The configuration for an alarm may also require an acknowledgment password. If this is the case the operator will be prompted only once for the password (for each type of alarm).

**Delete an Alarm**

1. In the Main Alarm Monitoring window, highlight (click) the alarm you wish to delete.
2. Complete one of the following:
   - Press the <Delete> key.
   - From the *Edit* menu select *Delete*.
3. A confirmation message displays. Click [Yes].

**Delete All Alarms**

Depending on how your System Administrator configured alarms, some alarms cannot be deleted until they have been acknowledged. OnGuard will alert you if this is the case.

1. To delete all of the alarm entries from the current alarm view, select *Delete All* from the *Edit* menu.
2. A confirmation message displays. Click [Yes]. All entries will be removed from the Main Alarm Monitoring window.

**Display a Map**

*A monitoring map* is a graphical representation of a facility or area monitored by the system. You can manually view maps associated with an alarm or you can set your display options to automatically display maps when an alarm occurs.

1. To manually display a map, open Alarm Monitoring.
2. If alarms are displayed in the Main Alarm Monitor window, right-click an alarm that has a map associated with it and select *View Map*. Otherwise, with the alarm selected choose *Map* from the *View* menu.
3. If no alarms are displayed in the Main Alarm Monitor window, select *Map Selection* from the *View* menu. Select the desired map and click [OK].

**Note:** If the selected device has multiple maps associated with it you will be prompted to select a map from a list provided. Do so and click [OK].
Example of a Map

Graphical symbols on the map indicate the location of devices. Using your mouse, scroll over each symbol to view the device status and any text associated with the device. For information on associating text with map icons refer to the MapDesigner User Guide.

Right-click a device symbol to perform a variety of operations depending on the type of device you select.

The word “ALARM” blinks, indicating an alarm’s location on the map.

- The blinking alarm displays only if there is one or more alarm designated as an “Active Alarm” in the System Administration software and if these alarms are unacknowledged/undeleted.
- An alarm sprite is a small bitmap image used as an icon. It disappears once the alarm has been acknowledged.
- The alarm sprite disappears if the alarm has been deleted without acknowledgment (as in the case of an initiating alarm that is automatically replaced by a canceling alarm).
- The alarm sprite is not used for canceling alarms.

View Linked Maps

Several maps can be linked to each other using the MapDesigner software application. For more information refer to the “Place Icons on a background” section in the MapDesigner User Guide.

To view linked maps do one of the following:

- If the map that is currently displayed has a link to another map, you can double-click the icon or right-click and select Switch Map.
- With a map currently displayed, click the map icon beside the File menu option. If you have previously brought up more than one map, a Back 1 Map menu option displays. If you go back one map, a Forward 1 Map menu option displays.
Send an E-mail

Using OnGuard software you can automatically or manually send electronic mail with alarm information. Contact your System Administrator to automatically send electronic mail for specific alarms.

To manually send an e-mail using Alarm Monitoring:

1. Verify the Global Output Server is running by clicking Start and selecting *Programs > OnGuard 2013 > Service and Support > Service and Support > Global Output Server.*
2. Right-click an alarm and select *Send Email.* The Send Email window opens.
3. Click [To] and select (place a checkmark beside) the desired e-mail addresses. Use the <Ctrl> or the <Shift> key to select multiple addresses.
4. The subject and body of the message are automatically populated with information that describes the alarm. Click in either field to make any changes.
5. Click [OK].

**To**

Allows you to select an e-mail address that is already in the database.

**Subject**

Displays the subject of the message. By default, the description of the alarm that has occurred is displayed. To change it, type over the text.

**Message**

Displays the body of the message being sent. By default, information pertaining to the alarm is displayed. To change it, type over the text.
**OK**
Once you are done, click the [OK] button to send the message and exit the window.

**Cancel**
To exit the window without sending an e-mail message, click the [Cancel] button.

**Send a Page**
Using OnGuard software you can send a page to a recipient with alarm information.

1. Verify the Global Output Server is running by clicking Start and selecting Programs > OnGuard 2013 > Service and Support > Global Output Server.
2. Right-click an alarm and select **Send Page**. The Send Page window opens.
3. Click [To] and select (place a checkmark beside) the pager number of the recipient.
4. The message field is automatically populated with an alarm description, the time and date on which it occurred and the location (which reader/alarm panel).
5. Click [OK] to send the page.

**To**
Allows you to select pager number that is already in the database.

**Message**
Displays the body of the message being sent. By default, information pertaining to the alarm is displayed. To change it, type over the text.

**OK**
Once you are done, click the [OK] button to send the message and exit the window.

**Cancel**
To exit the window without sending a page, click the [Cancel] button.
**CHAPTER 14**

**Muster Mode**

*Mustering* is a licensed feature that identifies all cardholders in a hazardous location during an incident. When an incident occurs (triggers an alarm) OnGuard automatically goes into muster mode. System operators can also manually initiate muster mode if necessary.

An **incident** is any situation/emergency where everyone in a hazardous area must evacuate and convene at designated safe locations. Safe locations are defined by exit and entry readers called muster readers. These readers are used purely for registration purposes and not to actually gain access into the safe location.

When an incident occurs a muster report can be generated listing all personnel within a hazardous location. During an incident cardholders must register in a safe location by entering the safe location via a designated muster readers. Registering in a safe location removes the cardholder from the muster report. In this way the muster report becomes a report of all those who are on-site and have failed to register in a safe location.

At the end of an incident system operators can remove all cardholders from the safe locations; this is referred to as a **muster reset**.

**Overview of Hazardous/Safe Locations**

Hazardous and safe locations are defined in System Administration as a special type of global APB (Anti-PassBack) area. **APB** is the prevention of a badge from gaining entry in an access control system when that badge has either recently entered the same reader or area (timed APB) or is not considered to be in the proper area required to gain entry into a new area (area APB). **Global APB** is APB enforced at a system level; areas span across multiple controllers.

Global APB can be soft APB or hard. **Soft APB** allows badges to enter areas that would normally be denied due to APB violations whereas **Hard APB** does not.

**Hard APB in Hazardous Locations**

Soft global APB is required for hazardous locations but it is strongly recommended that hard global APB be used when ever possible, because soft global APB can invalidate the accuracy of muster reporting. For example the accuracy of muster reporting will be compromised if a person swipes into
a hazardous location that they are already considered to be in or swipes out of a hazardous location when they are not considered to be in it.

Note: Soft global APB is required for hazardous locations but it is strongly recommended that hard global APB be used when ever possible.

Soft APB in Safe Locations

Soft APB must be applied to safe locations. It is assumed that readers entering safe locations are used purely for registration purposes and not to actually gain access into the safe location. In other words it is not expected that a badge will be presented to a reader to register at a safe location except during a muster mode. Since readers entering safe locations are used purely for registration purposes and not to gain access, any card transaction at a reader entering a safe location that contains a badge ID will be used to register that badge as being in a safe location. This includes granted with entry, granted with no entry, and access denied transactions.

Note: Soft Global APB is required for safe locations.

Enable Global APB

Hazardous and safe locations are segmented and can only belong to one segment at any time. In order to enable mustering functionality in a given segment, Global APB support must be enabled in that segment.

To enable global APB:

- In a segmented system, open System Administration or ID CredentialCenter and 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, open System Administration or ID CredentialCenter and select Administration > System Options. Select the Global Anti-Passback check box on the Anti-Passback form.

Mustering Inside Hazardous Locations

For every hazardous location there must be at least one safe location associated with it, although multiple safe locations can be specified. In addition, multiple APB areas can be defined as hazardous, and safe locations can exist within these hazardous locations. Refer to the following example.
This site wants to do mustering inside of a hazardous location. They also want to use APB within area 1 (hazardous location) and the two storage rooms (area 2 and area 3). To have APB control within the two storage rooms, area 2 and area 3 must be defined as separate areas.

When a Badge enters “Storage Room B”, the system will consider it to be area 3. As far as APB goes, that person is not considered to be in area 1 (the hazardous location). To function properly in this situation APB will not allow the badge to re-enter area 1 through any reader other than a reader leaving area 3.

However, for purposes of mustering, a person in “Storage Room B” (area 3) or in “Storage Room A” (area 2) needs to be considered as being in a hazardous location since everything inside of Building 1 except the safe location (area 4) is in the danger zone.

How can both of these be achieved? The answer is by considering the hazardous location to be a combination of area 1 + area 2 + area 3. When determining who is in the hazardous location, mustering will report anybody who is currently in any one of those areas.

Only normal APB areas can be configured as being contained in a hazardous location. Safe locations cannot, even though they may physically reside inside the hazardous location. This is because Badges recorded in a safe location should not be considered as being contained in the hazardous location.
General Constraints of Muster Mode

- When controllers go offline, OnGuard is not able to provide accurate muster and safe location reports since OnGuard will be unaware of access activity and safe location registration that occurs while a controller is offline. When the controller comes back online, OnGuard will be able to synchronize as long as the controller queued up all event transactions while it was offline.

Note: It is recommended that dual path panels and communications be deployed to help avoid offline panel situations.

- For the case of safe areas outside of hazardous areas, the muster exit readers are unlocked providing free access into and out of the hazardous area. Therefore access into and out of hazardous areas during an incident cannot be accurately tracked. Registration at the safe locations is what is accurately tracked.

Note: For the case of safe locations inside of hazardous areas, entry and exit readers are locked.

Recommendations for Optimal Reliability

- The operators main concern during an incident is to change the mode of muster exit readers to unlocked or locked and to run the muster and safe location reports.

- If a reader entering or leaving a hazardous location is configured with an offline mode of “unlocked” or “facility code only” and that reader goes offline with the controller, badges will be able to enter and/or exit the hazardous location without a record being made. If an incident occurs before these badges are swiped again (thus self-correcting the record of their location), the muster report will not be correct. It may list badges as being in hazardous locations when they are no longer there. Furthermore, it may not list badges that are still in the hazardous location as being there.

The same issues can occur if, during normal times, badges are not forced to swipe at muster readers to gain entry into and out of hazardous areas or if physical barriers are not present to enforce one and only one physical entry per card swipe.

Lenel recommends the following during normal times, at muster entry and exit readers:

- Require that all access to hazardous locations be performed through the Access Control System. Utilize physical barriers such as full turnstile and vehicle gates to enforce one and only one physical entry per card swipe.

  This implies that a scenario should not be allowed where people freely enter a hazardous location and are then issued an access control badge once inside. If an incident occurs just after they have entered the hazardous location, there will be no record of them being in the hazardous area. If personnel, such as visitors, must enter hazardous locations without being issued a physical badge, they should first be issued a “virtual” badge in the system and the interface to manually place their badges inside of the hazardous location should be used. When they visitors physically leave the hazardous location, the same interface should be used to manually take them out of the hazardous location. It is likely going to be simpler and more reliable to actually issue real visitor badges that are used for access into and out of the hazardous locations.

- Utilize Hard APB enforcement into and out of hazardous locations.

- Configure reader offline modes to be “Locked”. If personnel must enter/exit the hazardous areas through doors whose readers are currently offline with their ISC, record the badge
movement via the interface for manually moving a badge into a specific area. Note, however, that if free access is required through muster exit readers during muster mode, that the door strikes must be physically overridden during muster mode via an external source to ensure free exit during muster mode when readers are offline with their ISC’s.

Additionally, all host computers running OnGuard Communication Servers that are communicating with Access Controllers in the same Global APB Segment, must be time synchronized.

- OnGuard will not automatically change the mode of muster exit readers to unlocked or locked during an incident and back to a card mode at the end of an incident. It is assumed an external override will be used to override door strikes and physical barriers. For example if a fire system and access control system are installed at a site, the access control system is typically not depended upon to unlock the doors during a fire; the fire system overrides the door strike.
- Registration at safe locations is required after muster mode occurs even if personnel are already in the safe location at the start of the incident.

### Muster Mode in Main Alarm Monitoring Window

In muster mode, the Main Alarm Monitoring window displays a muster mode start alarm. Right-clicking the alarm and selecting the area in muster mode displays a sub-menu of options. These options are also available by right-clicking a hazardous or safe area icon in a map or in the System Status window.

**Note:** In certain situations some right-click options listed below may not be available because they are location and/or mode (normal or muster) dependant.

#### Right-click Muster mode alarm sub-menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Area Status</td>
<td>Updates the status of both safe and hazardous areas so that operators can have a current view of cardholder locations.</td>
</tr>
<tr>
<td>View Map</td>
<td>Displays a map associated with the alarm. If several maps are associated with an alarm, the operator is prompted to select a map.</td>
</tr>
<tr>
<td>Move Badges</td>
<td>Enables an operator to manually move all the badges in one area to another.</td>
</tr>
<tr>
<td>Occupancy Report</td>
<td>Provides a current report of the cardholders currently in a safe area with information such as: the badge ID, the cardholder name, the time entered, and how the area was entered.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The occupancy report can also be run for a hazardous area. The occupancy report for a hazardous area is similar to the muster report except it does not report the last attempted location.</td>
</tr>
<tr>
<td>Muster Report</td>
<td>Provides a current report of the cardholders currently in a safe area with information such as: the badge ID, the cardholder name, the time entered, and the area/last attempted location.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The muster report cannot be run for a safe area.</td>
</tr>
<tr>
<td>Start Muster Mode</td>
<td>Initiates muster mode. The Start Muster Mode window displays and provides an area to enter comments.</td>
</tr>
</tbody>
</table>
Right-click Muster mode alarm sub-menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Muster Mode</td>
<td>Ends muster mode. The Reset Muster Mode window displays and provides an area to enter comments.</td>
</tr>
</tbody>
</table>

Hazardous / Safe Locations in System Status Window

Hazardous and safe location icons display in the System Status window under the Global Anti-Passback Areas and Mustering section. Alarm monitoring operators can right-click hazardous or safe area icons and view all or some of the options available in the Right-click Muster mode alarm sub-menu options on page 169 table, depending on the area selected.

Muster Mode Procedures

Use the following procedures for muster mode.

Initiate Muster Mode

Muster mode is manually initiated via the Main Alarm Monitoring window, System Status window or map view. Depending on how your System Administrator configures hazardous locations, muster mode initiation may automatically remove all cardholders from a safe location.

1. Using the Alarm Monitoring application, do one of the following:
   - From the Main Alarm Monitoring window - Right-click the Muster Mode Start alarm and select the hazardous location in muster mode. A sub-menu displays. Select Start Muster Mode.
   - From the System Status window - Right-click an area and select Start Muster Mode.
   - From the View menu select Map - Right-click a hazardous area and select Start Muster Mode.

2. The Start Muster Mode window displays.
3. Enter any notes relating to why muster mode is being activated, and click [Yes] to activate muster mode.

4. A warning message displays. Click [OK]. Muster mode is initiated.

**Reset Muster Mode**

Muster reset is a manual operation that takes a hazardous area out of muster mode. Muster reset will not automatically remove personnel in hazardous locations. If a person really does remain in a hazardous area, you want to keep a record of them being there.

1. Using the Alarm Monitoring application, do one of the following:
   - From the Main Alarm Monitoring window - Right-click the Muster Mode Start alarm and select the hazardous location in muster mode. A sub-menu displays. Select **Reset Muster Mode**.
   - From the System Status window - Right-click an area and select **Reset Muster Mode**.
   - From the **View** menu select **Map**. Right-click a hazardous area and select **Reset Muster Mode**.

2. The Reset Muster Mode window displays. Enter any notes and click [Yes] to reset muster mode.

3. A warning message displays. Click [OK] and muster mode is initiated.

**Reports**

Several reports are available with mustering:

- **Muster mode report** - lists the badge IDs, cardholder name, time entered, how entered, and their last attempted location for a specific hazardous area. The status bar of the report displays the total occupancy for that area and the words MUSTER MODE. The title of the report displays the name of hazardous location and the time and date the report was initiated.
- **Occupancy report** - list badge IDs, cardholder name, time entered, and how entered. The status bar displays the total occupancy for that area. The title of the report displays the name of the safe location and the time and date the report was initiated. The occupancy report is sometimes referred to as the Safe Location report.
Run Muster and Occupancy Reports

Operators can run the muster and occupancy reports from the Main Alarm Monitoring window or System Status window. They can also right-click a hazardous or safe icon in map view to run reports.

1. Display either the Main Alarm Monitoring window or the System Status window.
2. Do one of the following:
   - From the Main Alarm Monitoring window - Right-click the Muster Mode Start alarm, select the device (in this case it would be the hazardous location in muster mode.) A sub-menu displays. Select Muster Report or Occupancy Report.
   - From the System Status window - Right-click an area and select Muster Report or Occupancy Report.

Notes: Muster reporting automatically refreshes every two minutes. However the user can manually refresh a report at any time.

Automatic reporting ends when the number of personnel in the muster report becomes zero.

Report right-click options

Both the muster and occupancy report (via right-click options) allow operators to move one or several badges from an area as well as select a cardholder and bring up their badge information.

Moving Badges

The focus of muster mode is to account for all personnel in hazardous locations. The muster report provides this information. If an operator verifies that personnel recorded as being in the hazardous location are physically outside the hazardous area they can manually move the badge to a different area.

Move All Badges from an Area

1. You can move every badge from a safe or hazardous area via several windows:
   - From the Main Alarm Monitoring window right-click the muster mode Start alarm, select the hazardous area and then select Move Badges.
   - From the System Status window right-click an APB area and select Move Badges.
   - From a map view right-click an APB area and select Move Badges.
2. When prompted to confirm your request. Click [Yes].
3. The Area Move Badges window displays. Select the desired area (a checkmark displays beside the area), enter any notes and click [OK].
Operators can also move a single badge from a safe or hazardous area; this can only be done through the occupancy or muster report.

1. Run the occupancy or muster report. For more information, refer to Run Muster and Occupancy Reports on page 172.
2. From the occupancy or muster report right-click and select Move Badge to APB Area.

**Note:** You can also move multiple badges from an area; this can be done by highlighting the desired badges, right-clicking and selecting Move Badge to APB area.
Advanced Operator Procedures
CHAPTER 15

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 Badge Info from the View 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.
Cardholders Folder

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo display</td>
<td>Displays the cardholder’s photo as it appears on their badge.</td>
</tr>
<tr>
<td>Signature display</td>
<td>Displays the cardholder’s signature as it appears on their badge.</td>
</tr>
<tr>
<td>Last access</td>
<td>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.</td>
</tr>
<tr>
<td>Badge ID</td>
<td>Displays the numeric identifier assigned to the cardholder’s active badge.</td>
</tr>
<tr>
<td>Issue code</td>
<td>Displays the issue code assigned to the cardholder’s active badge.</td>
</tr>
<tr>
<td>Prints</td>
<td>Displays the number of times the active badge has been printed.</td>
</tr>
<tr>
<td>Activate</td>
<td>Displays the date when the badge becomes valid.</td>
</tr>
<tr>
<td>Deactivate</td>
<td>Displays the date when the badge becomes invalid.</td>
</tr>
<tr>
<td>Last name</td>
<td>Indicates the cardholder’s last name.</td>
</tr>
<tr>
<td>First name</td>
<td>Indicates the cardholder’s first name.</td>
</tr>
<tr>
<td>Middle name</td>
<td>Indicates the cardholder’s middle name.</td>
</tr>
<tr>
<td>Cardholder ID</td>
<td>Indicates the cardholder’s ID number. This field is not displayed on the Visitor form.</td>
</tr>
</tbody>
</table>
Cardholders Folder Fields

**Badge type**
Indicates the cardholder’s badge type. Badge types are configured in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.

**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 20: Print Report Options Window on page 321.

**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 the Card Formats Folder chapter in the System Administration User Guide. 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 (Cardholder Sub-tab) in the System Administration or ID CredentialCenter user guide.

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.

<table>
<thead>
<tr>
<th>Comparison operator</th>
<th>Description</th>
<th>Text field</th>
<th>Numeric field</th>
<th>Drop-down list</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equal to</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>!= or &lt;&gt;</td>
<td>Not equal to</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
</tbody>
</table>
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 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:
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 manner, 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

1. **Scan badge**

2. **Is CAC being used?**
   - **No**
   - **Yes**

3. **Is length of number scanned greater than Limit?**
   - **No**
   - **Yes**

4. **OnGuard decrypts social security number from CAC number**
5. **OnGuard searches up social security number**
6. **OnGuard examines **Field** and **Table**

---

**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.
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.

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.
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 194 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 194 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 in System Administration.

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 the Cardholder Options chapter in the System Administration User Guide.
   b. Ensure the PIV card is inserted in the PC/SC encoder/scanner.

### Cardholder/Visitor Import

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

### 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 190 and Import Fingerprints from a PIV Card on page 191.

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 192.

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 194.
Cardholder Form Procedures

The following procedures can be performed on the Cardholder form.

Add a Cardholder Record

1. Select Badge Info choice the View 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 refer to the Multimedia Capture appendix in the System Administration User Guide.
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.

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.
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:

   ![Delete Confirmation Message]

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:

   ![Destroy Confirmation Message]

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 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 193.

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].

Add a Visitor Record
1. Select the Badge Info from the View 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.

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. For more information refer to the Segments Folder chapter in the System Administration User Guide.

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 the **Badge Info** from the **View** 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.
   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 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.
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 205.

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.

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.
Badge Form

**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.
For more information, refer to the Destination Assurance Folder chapter in the System Administration User Guide.

**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 ILS Integra Locks” and “Configure Special Purpose Cards for ILS Offline/Wireless Locks” in the System Administration User Guide.

**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.

**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.

**Allow Access To**
Displayed only when a valid guest class badge type is selected. Valid guest class badge types are those badge types which were configured during their creation to provide guest parameters.
Choices in the drop-down list include readers/locks that are associated with the selected badge type. Select an option from the list if you want to assign the selected cardholder to a specific guest reader/lock.
The Badge ID and Issue Code fields are automatically updated when a cardholder is assigned to a guest reader/lock. The values for these fields are obtained from the next available badge ID from the badge numbers reserved for the selected reader, and the next valid issue code for that badge
number. The values are updated after you select an item for the drop-down list and then move on to another field on the form. This field is subject to licensing restrictions.

**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. For more information, refer to the Command Keypad Templates Folder in the System Administration User Guide.
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 the Badge Info from the View 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:
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

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 previous and next 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:
   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 in the System Administration User Guide.

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 in the System Administration User Guide.

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
1. 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 in the System Administration software application.
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 the Badge Info from the View 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 refer to Multimedia Capture appendix in the System Administration User Guide.

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 the **Badge Info** from the **View** 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)](image-url)
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 the **Badge Info** from the **View** menu.
2. Click the Cardholders tab.
3. Locate the record of the cardholder that you want to allow visitors.
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

![Assets Form](image)

**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 the Badge Info from the View 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 the Badge Info from the View 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].

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. For more information refer to the Guard Tour Folder chapter in the System Administration User Guide.

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 the Badge Info from the View 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.

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 the Badge Info from the View 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.


**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 (View Mode)](image1)

*ILS Authorization Form (Modify Mode)*

![ILS Authorization Form (Modify Mode)](image2)
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 the Lenel (Integrated Locking Solutions) appendix in the System Administration User Guide.
CHAPTER 16  

**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, displaying 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.
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.

• 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.
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 View menu.

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 241. For descriptions of the unique form elements refer to Status Search Form on page 256, Visit Form on page 254, Details Form on page 258, and E-mail Form on page 258, and Reports Form on page 261.
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 in the Cardholder Options Folder chapter in the System Administration User Guide.

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
Visits Folder

- **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 the Cardholder Options Folder chapter in the System Administration User Guide.
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 displayed 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.
Visits Folder Fields

- Automatic sign in is enabled. For more information about this feature, refer to the Automatic Sign In section of the Visitor Management User Guide.

![Sign In Visit(s) window](image)

**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 the rights to access to the Choose alternate printer option via the Users Folder, Cardholder Permission Groups Form. For more information refer to the Users Folder chapter in the System Administration or ID CredentialCenter users guide. 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 the Users Folder chapter in the System Administration or ID CredentialCenter users guide. 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.

<table>
<thead>
<tr>
<th>Comparison operator</th>
<th>Description</th>
<th>Text field</th>
<th>Numeric field</th>
<th>Drop-down list</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equal to</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>!= or &lt;&gt;</td>
<td>Not equal to</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>%</td>
<td>Contains</td>
<td>Yes</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

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 begins 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 **View** 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 **View** 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 **View** 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.
visits folder procedures

- 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 **View** 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.

   ![Scheduled time in:](image)

   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.

   ![Scheduled time in:](image)

   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 View 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.

Note: This procedure does not apply to view/edit only workstations.

1. Select Visits from the View 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 263.
      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 264.

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 266.

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 258. 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 in System Administration or ID CredentialCenter by selecting the Administration menu, then selecting List Builder.

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 258. 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 263.
- 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 265.
- 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 in System Administration. 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 in System Administration.
   - 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

**Note:** This procedure does not apply to view only workstations.

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. Locate the visit record you want to change and select it in the Visits listing window.
Visits Folder

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

Note: This procedure does not apply to view/edit only workstations.

1. Select Visits from the View 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 View 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 in System Administration 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

Note: This procedure does not apply to view only workstations.
Visits Folder Procedures

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 248.
   b. Search for an existing visit and click [Sign In]. For more information, refer to Search for Scheduled, Active or Finished Visits on page 246.

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

Note: This procedure does not apply to view only workstations.

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” in the Cardholder Options Folder in the System Administration User Guide.

1. Select Visits from the View 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
etime 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.

![Image of Details form]

**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 the List Builder Folder chapter in the System Administration User Guide.

**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
E-mail Form

**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 263.

**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 263.

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 265.

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 in the System Administration User Guide.

**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.

Note: This procedure does not apply to view only workstations.

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 View 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 244
      • Search for All Visits to a Selected Cardholder on page 245
      • Search for All Visits by a Selected Visitor on page 246
      • Search for Scheduled, Active or Finished Visits on page 246
      • Search for All Visits for a Specific Date or Time on page 247
      • Retrieve the Most Recent Visit Search Results on page 248
   
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 View 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.

   ![Print Report Options window](image)

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 the Segments Folder chapter in the System Administration User Guide.

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 the Badge Types Folder chapter in the System Administration User Guide.

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 Wizard: Select or Add Form

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 the Badge Types Folder chapter in the System Administration User Guide.

**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 18

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 the Asset Info from the View menu.

Toolbar Shortcut

Assets
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.
Assets Form

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 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 the Asset Type form.

**Asset Subtype**

In add or modify 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

Note: This procedure does not apply to view/edit only workstations.

1. Select **Asset Info** from the **View** 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 refer to the Multimedia Capture appendix in the System Administration User Guide.
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 281.
13. Click **[OK]**.

Modify an Asset

Note: This procedure does not apply to view only workstations.

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

Note: This procedure does not apply to view/edit only workstations.

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

Assign a Cardholder to an Asset

Note: This procedure does not apply to view only workstations.
Assets Form Procedures

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 Asset Info from the View 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

Note: This procedure does not apply to view only workstations.
1. Select Asset Info from the View 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)*
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.
Asset Classes Form Procedures

The following procedures can be performed on this form.

Assign Classes to an Asset

Note: This procedure does not apply to view only workstations.

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

Note: This procedure does not apply to view only workstations.

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 Asset Info from the View 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 button to remove the asset group. Click the button to 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.
Assignments Form

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 to 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.
Assignments Form Procedures

The following procedures can be performed on this form.

Assign a Cardholder to an Asset

Note: This procedure does not apply to view only workstations.

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

Note: This procedure does not apply to view only workstations.

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

**Note:** The Reports form is not available in view/edit only workstations or in the Alarm Monitoring application.

![Image of Reports Form](image)

**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

Note: This procedure does not apply to Alarm Monitoring.
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 the Report Print Preview Window chapter in the System Administration User Guide.
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 View 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 C: Reports on page 487.
**Report Configuration Form**

![Report Configuration Form](image)

**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.

**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.

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.

Guest
If this checkbox is selected, guest 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 View 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
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 327.

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 \( \text{ } \) and \( \text{ } \) 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 \( \text{ } \).

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.
Reader Reports Form

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 2003.

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 the Archives Folder in the System Administration User Guide.

**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 *View* 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 21: Report Print Preview Window* on page 325.

**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 ⬠ and ⬡.

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.

![Start time](image)

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.

![Calendar](image)

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.

![End time](image)

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 the Archives Folder chapter
in the System Administration User Guide.

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 View 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 21: Report Print Preview Window on page 325.

**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.
Anti-Passback Reports Form

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 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 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.
Anti-Passback Reports Form Procedures

The following procedures can be performed on this form.

Run an Anti-Passback Report

1. Select Reports from the View 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 21: Report Print Preview Window on page 325.

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.

![Check box for 208:02 AM]

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.

![Calendar for April 2003]

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.

![Check box for 208:02 AM]

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 the Archives Folder chapter in the System Administration User Guide.
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 View 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 21: Report Print Preview Window on page 325.

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.
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 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 the Archives Folder chapter in the System Administration User Guide.

**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 View 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 21: Report Print Preview Window on page 325.

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 the Archives Folder chapter in the System Administration User Guide.

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 View 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 21: Report Print Preview Window on page 325.

**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.

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 the Archives Folder chapter in the System Administration User Guide.

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 *View* 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 21: Report Print Preview Window on page 325.

**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 20

Print Report Options Window

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 on the Reports form or the Print toolbar button while a report is displayed.

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 21: Report Print Preview Window on page 325.

**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. Reports are also available in the Cardholders folder (Reports form) and the Assets folder (Reports form). You can use this procedure to print those reports as well.

**Notes:**
The report form is available from within the Reports folder, Cardholders folder and Assets folder for System Administration and ID CredentialCenter.
The report form is only available from the Cardholders folder in Alarm Monitoring. (View > Badge Info > Reports form/tab).
The availability of the Reports folder is subject to licensing restrictions.
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 on the Main toolbar
   - [Print] button on the form
4. Select a report from within the Reports folder.
5. The Print Report Options window opens.
6. In the Print Destination section, select whether to print to a preview window, export directly to a file or print directly to a printer.
7. 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.

8. In the Report Subtitle section, type the report subtitle. The subtitle will be displayed below the report title on the report.
9. Click [OK]. The options selected in the Print Destination section will determine where the report is sent.
• 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] , the report is automatically printed to the Report Print Preview window.

This window is displayed by:
• Clicking [Print] , selecting the Print to a Preview Window radio button on the Print Report Options window, then clicking the [OK] button.

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 327.

**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.
Report Print Preview Window Procedures

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.
2. Click one of the following:
   - The [Print] button, select the Print to a Preview Window radio button and then click [OK].
   - The [Preview] button.
3. 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.
4. Use the ‹, ‡, † and ‡ buttons or the <Page Down>/<Page Up> keys to view other pages of the report.

5. 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.

6. 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.

7. 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.
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.)

Guard tour records the location and timestamp for each checkpoint visited by the tour 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 overdue. A late event means the checkpoint was reached after its maximum time expired. An overdue event means the checkpoint has not yet been reached.

A tour is considered complete when one of the following actions occurs:

- All of the checkpoints on the tour are reached, even if they are reached out of sequence or some checkpoints are missed
- The tour is acknowledged as complete at a monitoring station
- The tour is terminated at a monitoring station

Note: System Administrator procedures to set up a Guard Tour are located in the Guard Tour Folder chapter in the System Administration User Guide.
Start Guard Tour Form

Select Tour listing window
Displays a list of configured Guard Tours. Click a tour to select it. A checkmark displays beside a tour when it is selected.

Select Guard
Displays a list of guards. Select a guard to perform the Guard Tour. The list of Guards can be filtered by selecting the show guards with proper security clearance level radio button.

Show guards with proper security clearance level
Limits the guards displayed in the Select guard listing to the guards with authorization to perform the selected guard tour.

Show all guards
Displays all the guards in the Select guard listing.

Enter badge ID Manually
Provides you the option to enter the badge ID of the guard instead of selecting a guard from the Select guard list.

Tour Instructions
Displays the Tour Instructions window which contains specific instructions for the selected tour. From the Tour Instructions window you can print the instructions.
**Guard Tour Live Tracking Form**

<table>
<thead>
<tr>
<th>ID</th>
<th>Device</th>
<th>Checkpoint Status</th>
<th>Min. Time</th>
<th>Max. Time</th>
<th>Actual Time</th>
<th>Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reader 1</td>
<td>Checkpoint not reached</td>
<td>30s, 6s</td>
<td>1min, 6s</td>
<td>00s, 6s</td>
<td>Access Panel 2000</td>
</tr>
</tbody>
</table>

**Terminate**

Stops a tour before it is completed (before all of the checkpoints have been reached). When this button is selected, a “Guard Tour Terminated” event is generated.

**Force Complete**

Manually completes a tour. For example, the [Force Complete] button could be used to end a tour that otherwise could not be completed because of a card that could not be swiped at a reader (a checkpoint) that was in “unlocked” mode.

**View Instructions**

Displays special instructions that were written for this tour when it was configured in the System Administration application.

**Add Tour Note**

Adds a note to an event. For example, you can add a note explaining why a particular checkpoint was reached late.

**Show Video**

Displays live video of the tour as it progresses. (This button is displayed only when the tour is configured to show video.)

**Guard Tour Events**

- **Guard Tour Initiated**
  
  Generated when a tour is launched from a monitoring station.

- **Guard Tour Completed**
  
  Generated when all checkpoints on a tour have a “Checkpoint Reached on Time” status. Otherwise, a “Guard Tour Completed with Errors” event is generated.
Guard Tour Completed with Errors
Generated when the last checkpoint has been reached but one or more checkpoints were not reached on time or were missed altogether.

Guard Tour Cancelled
Generated when the scheduled automatic guard tour is cancelled before the tour was started.

Guard Tour Terminated
Generated when the [Terminate] button is selected in the Guard Tour Live Tracking window.

Checkpoint reached out of Sequence
Generated when a checkpoint is hit ahead of schedule on a tour (i.e., it is supposed to be hit later in a tour).

Checkpoint Missed
When a checkpoint is assigned a status of “Checkpoint reached out of sequence”, the “Checkpoint Missed” event is generated for all previous checkpoints that have a status of “Checkpoint Not Reached.”

Checkpoint Reached on Time
Generated when a checkpoint is hit between its minimum and maximum checkpoint times.
Checkpoint reached events are generated when any inputs that are used as checkpoints are activated.

Checkpoint Reached Early
Generated when a checkpoint is the next checkpoint on a tour and is hit before its minimum checkpoint time has elapsed.
Checkpoint reached events are generated when any inputs that are used as checkpoints are activated.

Checkpoint Overdue
Generated when a checkpoint’s maximum checkpoint time has elapsed and the guard has not yet arrived.

Checkpoint Reached Late
Generated for a checkpoint when its maximum checkpoint time has elapsed and it is then hit.
Checkpoint reached events are generated when any inputs that are used as checkpoints are activated.

Guard Tour Form Procedures
Use the following procedures on this form.

Launch a Guard Tour
1. Start the Linkage Server by clicking the Start button, then selecting Programs > OnGuard 2013 > Service and Support > Linkage Server.
2. Open the Select Guard Tour window by completing one of the following:
   • From the Control menu, select Guard Tour > Launch.
Guard Tour Form Procedures

 Toolbar Shortcut

- Click the down arrow on the Guard Tour toolbar button and select Launch Tour.
- Right-click a tour name in the system status tree and select Launch Tour.

3. Select a tour in the Tour listing window.

Note: You can click [Tour Instructions] to see if any special instructions exist for this tour. These instructions are written when the tour is configured in System Administration.

4. If you know the badge ID of the tour guard, select the Enter badge ID manually radio button and type in their ID.
Otherwise select the Select guard radio button and complete the following:
   a. Select the Show guards with proper security clearance level radio button to limit the number of tour guards to choose from or select the Show all guards radio button to list all tour guards, regardless of their security clearance levels.
   b. Click a tour guard entry in the Name listing window to select it.

5. Click [OK]. The Guard Tour Live Tracking window opens.
6. At this time, the tour guard can begin the tour. As the tour progresses, the status of checkpoints and generated events display in the Guard Tour Live Tracking window. For more information, refer to Guard Tour Events on page 331.

Note: Checkpoints can be predecessors or successors. A predecessor checkpoint is any checkpoint occurring before other checkpoints on a tour. For example: a tour has three stops. Checkpoints one and two are the predecessors to checkpoint three. A successor checkpoint is any checkpoint occurring after other checkpoints on a tour. For example: a tour has three stops. Checkpoints two and three are successors to checkpoint one.

7. When a tour is completed, the Guard Tour Live Tracking window displays the status of the tour and the events that were generated.

Schedule an Automatic Guard Tour Action

Assuming your System Administrator has configured a Guard Tour (in System Administration) you can schedule an automatic guard tour action (in Alarm Monitoring). This means that using the Scheduler you can set OnGuard to automatically launch a Guard Tour on at a specific date and time as well as on a regular basis.

1. Open the Scheduler by clicking the Scheduler toolbar button or selecting Scheduler from View menu.
2. Click [Add].
3. The Add Action Wizard window displays. In the Category pane select Action Types. In the Objects pane select Automatic Guard Tour.
4. Click [Next].
5. The Automatic Guard Tour Properties window displays. Select a tour or tour group.
6. Select the Monitoring stations to be notified.
7. Click the Schedule tab.
8. Select the World time zone.
9. If the automatic Guard Tour is a single occurrence select the **One time** radio button and set the start date and time.

10. If the automatic Guard Tour will occur several times click the **Recurring** radio button and click [Change].
   a. Set how often you want the Guard Tour to occur and the start and end dates.
   b. Click [OK].
   c. The frequency settings display in the in the Recurring pane on the schedule tab.

11. Click [OK].

### Respond to an Automatic Guard Tour

1. When an automatic Guard Tour is started, Alarm Monitoring displays a “Scheduler Action Executed” alarm and you prompts you to start the Guard Tour.

2. Click [OK].

3. The Start Guard Tour window displays with the guard tour name selected. Select the guard (person) to complete the tour by either selecting the guard from the list provided or entering the guard’s badge ID.

4. Click [OK].

5. While the Guard Tour is active you can monitor the Guard Tour status by selecting **Control > Guard Tour > View** from the main menu.

6. The Guard Tour Live Tracking window display information such as the badge ID of the person performing the Guard Tour, the checkpoint statuses, tour history as well as the ability to view instructions and video.

### View a Guard Tour

1. Start the Linkage Server by clicking the Start button, then selecting **Programs > OnGuard 2013 > Service and Support > Linkage Server**.

2. Open the Select Guard Tour window by completing one of the following:
   - From the **Control** menu, select **Guard Tour > Launch**.
   - Click the down arrow on the Guard Tour toolbar button and select **Launch Tour**.

3. The View Guard Tour window opens. Select the tour and click [OK].
CHAPTER 23

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 349.

This folder is displayed by selecting Scheduler from the View menu.

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 in System Administration.

Scheduler Form

Note:

Service status
List 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 View 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 the Action Group Library Folder chapter in the System Administration User Guide.

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.

   ![July 2004 Calendar](image)

   - 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.

   ![2003 Year](image)

   - 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.

   ![Edit Recurring Action Schedule](image)

   e. 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.

```
© Day 4 of every 6 month(s)
```

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 on the 2nd Tuesday of every 3rd month.

```
© The 2nd Tuesday of every 3 month(s)
```

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.

```
© Occurs once 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.

```
© Occurs every: 2 hour(s) Starting at: 09:00 AM Ending at: 05:00 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 349.
Display the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.

| Add Action… |
| Start Action |
| Stop Action |
| View Action History… |
| View Current Status… |
| Refresh Action |
| Delete Action |
| Modify Action |

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 Action… |
| Start Action |
| Stop Action |
| View Action History… |
| View Current Status… |
| Refresh All Actions |
| Delete Action |
| Modify Action |

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.
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.

![Action History Window]

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:

![Status Message]

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 349.
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.
Appendices
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 in System Administration or ID CredentialCenter.

**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
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:
   “MaxNumberOfActionThreads=<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.

**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 353.

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 23: Scheduler Folder on page 337.

**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.

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 the Global I/O Folder chapter in the System Administration User Guide.

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.

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 the Guard Tour Folder chapter in the System Administration User Guide.

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.
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 the Alarm Configuration Folder chapter in the System Administration User Guide.

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.

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 350.

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 23: Scheduler Folder on page 337.

Description

When adding or modifying an action group, you can enter a description of the action group that is being configured.
Action Group Properties Window Procedures

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 “Action Groups Overview” in the Action Group Library Folder chapter in the System Administration User Guide.

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 350.
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 the Action Group Library Folder chapter in the System Administration User Guide.
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].
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 350.

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 350.
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 350.

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 23: Scheduler Folder on page 337.

Listing window
Displays the following message: “<This action will archive/purge the database using current archive/purge configurations>”
**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 350.
2. Click [OK]. This action is now configured to archive/purge the database using your current archive/purge configurations. For more information, refer to the Archives Folder chapter in the System Administration User Guide.

## 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 350.
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 23: Scheduler Folder on page 337.

Listing window
Lists currently enabled intrusion areas. Intrusion areas are configured on the Areas form in the Intrusion Detection Configuration folder.

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 350.
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 358 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 350.
Automatic Guard Tour Properties Window

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.
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 350.

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 23: Scheduler Folder on page 337.

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 23: Scheduler Folder on page 337.

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 350.

![Change Network Video Password Properties Window](image)

**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 23: Scheduler Folder on page 337.

**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 Chapter 1: Introduction to Alarm Monitoring on page 21.

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 350.
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 350.
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 350.
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.
7. Click [OK] on the Change Network Video Password Properties window.
The following procedures can be performed on this form.

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 350.

Note: In segmented systems, the Action History/Guard Tour Event Purging action must be applied to all segments.

![Deactivate Badge Properties Window]

**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 350.

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.
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 350.

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 23: Scheduler Folder on page 337.

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 350.
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 350.

![Device Output Group Properties Window](image)

**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 23: Scheduler Folder on page 337.

**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 350.
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 350.
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 23: Scheduler Folder on page 337.

**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 350.
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 350.

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 23: Scheduler Folder on page 337.

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 350.
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 350.

![Execute Function List Properties Window](image)

**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 23: Scheduler Folder** on page 337.

**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 as 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.
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 350.
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 350.
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 350.
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 350.
Global APB System/Segment Reset Properties Window Procedures

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 350.
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.

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 350.

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 23: Scheduler Folder on page 337.

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 350.
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 350.

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 23: Scheduler Folder on page 337.

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 350.
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 350.
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 350.

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 23: Scheduler Folder on page 337.

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.
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 350.

![Muster Mode Initiation Properties Window](image)

**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 350.
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 23: Scheduler Folder on page 337.

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 350.
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 350.
Mask/Unmask Alarm Input for Group Properties Window

[Image]

**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.

**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 23: Scheduler Folder on page 337.
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 350.

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 350.

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 23: Scheduler Folder on page 337.
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 350.
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 350.

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 23: Scheduler Folder on page 337.

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 350.

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 350.

![Mask/Unmask Door Forced Open Properties Window](image)

**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 23: Scheduler Folder on page 337.
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 350.
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 350.

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 23: Scheduler Folder on page 337.

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 350.
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 350.
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 23: Scheduler Folder on page 337.

**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 350.

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 350.

![Mask/Unmask Door Held Open for Reader Group Properties](image)

**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 23: Scheduler Folder on page 337.

**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
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 350.
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].

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.

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 350.

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 23: Scheduler Folder on page 337.

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. For more information, refer to “Action Groups Overview” in the Action Group Library Folder chapter in the System Administration User Guide.

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 350.
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 350.
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 23: Scheduler Folder on page 337.

**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 350.
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 350.
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 23: Scheduler Folder on page 337.

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 350.
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 350.
Reader Mode Group Properties Window

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 23: Scheduler Folder on page 337.

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.
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 350.
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 350.
Reset Use Limit Properties Window

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 23: Scheduler Folder on page 337.

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 350.
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 350.
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 350.
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 350.
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 in the System Administration User Guide.

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 the Global Output Devices Folder chapter in the System Administration User Guide.

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.
Schedule Report Properties Window Procedures

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 404.

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 350.
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 350.

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 23: Scheduler Folder on page 337.

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 350.

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 350.

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 23: Scheduler Folder on page 337.

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.
Select Video Wall Layout Properties Window Procedures

**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 350.
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.

![Set Forwarding Station Properties](image)

**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.
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 350.
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 350.

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 350.
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 350.

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 23: Scheduler Folder on page 337.

Listing window
Lists currently enabled intrusion areas. Intrusion areas are configured on the Areas form in the Intrusion Detection Configuration folder.

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 350.

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].

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
4. Click this button to display online help for this window.
## APPENDIX B

**Alarm/Event Descriptions**

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
<th>Duress*</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Hour Alarm</td>
<td>24 Hour Alarm</td>
<td>Trouble</td>
<td>A 24 hour alarm condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>24 Hour Alarm Restore</td>
<td>24 Hour Alarm Restore</td>
<td>Trouble</td>
<td>A 24 hour alarm condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>24 Hour Auto Test</td>
<td>24 Hour Auto Test</td>
<td>Trouble</td>
<td>A 24 hour non-burglary alarm condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>24 Hour Non-Burglary Alarm</td>
<td>24 Hour Non-Burglary Alarm</td>
<td>Trouble</td>
<td>A 24 hour non-burglary alarm condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>24 Hour Report Closed</td>
<td>24 Hour Report Closed</td>
<td>Trouble</td>
<td>A 24 hour report on a closed zone</td>
<td></td>
</tr>
<tr>
<td>24 Hour Report Open</td>
<td>24 Hour Report Open</td>
<td>Trouble</td>
<td>A 24 hour report on an open zone</td>
<td></td>
</tr>
<tr>
<td>24 Hour Zone Bypassed</td>
<td>24 Hour Zone Bypassed</td>
<td>Trouble</td>
<td>A 24 hour zone has been bypassed.</td>
<td></td>
</tr>
<tr>
<td>24 Hour Zone Unbypassed</td>
<td>24 Hour Zone Unbypassed</td>
<td>Trouble</td>
<td>A 24 hour zone has been unbypassed.</td>
<td></td>
</tr>
<tr>
<td>30 Minutes Since Fallback Command</td>
<td>30 Minutes Since Fallback Command</td>
<td>Trouble</td>
<td>30 minutes have passed since fallback command.</td>
<td></td>
</tr>
<tr>
<td>32 Hour Event Log Marker</td>
<td>32 Hour Event Log Marker</td>
<td>System</td>
<td>An event message was not sent due to User action</td>
<td></td>
</tr>
<tr>
<td>Abort</td>
<td>Abort</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>AC Restore</td>
<td>AC Restore</td>
<td>System</td>
<td>AC power trouble has been restored.</td>
<td></td>
</tr>
<tr>
<td>AC Trouble</td>
<td>AC Trouble</td>
<td>System</td>
<td>An AC power trouble condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Accepted Biometric Score</td>
<td>Accepted Biometric Score</td>
<td>Biometric</td>
<td>This event returns the accepted biometric score. The actual access granted event is sent separately. This event is mainly used for diagnostic purposes.</td>
<td></td>
</tr>
<tr>
<td>Access Closed</td>
<td>Access Closed</td>
<td>Denied</td>
<td>Access for all users prohibited.</td>
<td></td>
</tr>
<tr>
<td>Access Code Used</td>
<td>Access Code Used</td>
<td>Denied</td>
<td>Access code was used.</td>
<td></td>
</tr>
<tr>
<td>Access Denied</td>
<td>Access Denied</td>
<td>Denied</td>
<td>Access was denied.</td>
<td></td>
</tr>
<tr>
<td>Access Denied to Destination Floor</td>
<td>Access Denied to Destination Floor</td>
<td>Denied</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Access Control Format Not Found</td>
<td>Access Denied: Access Control Format Not Found</td>
<td>Denied</td>
<td>Generated when there are no ACFs (Access Control Formats) stored at the lock.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Area Empty</td>
<td>Access Denied</td>
<td>Denied</td>
<td>An event indicating that access was denied due to the room being empty.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Denied: Area Occupied</td>
<td>Access Denied</td>
<td>Denied</td>
<td>An event indicating that access was denied due to the room being empty.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Denied: Asset Required</td>
<td>Access Denied</td>
<td>Denied</td>
<td>An event indicating that access was denied since no asset was presented for the access attempt.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Denied: Biometric Reader Offline</td>
<td>Access Denied: Biometric Reader Offline</td>
<td>Denied</td>
<td>Generated when the alternate biometric reader could not be contacted for verification (was offline).</td>
<td>Yes</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Access Denied: Escort Timeout Expired</td>
<td>Access Denied: Escort Timeout Expired</td>
<td>Denied</td>
<td>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.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Denied: Door Secured</td>
<td>Access Denied: Door Secured</td>
<td>Denied</td>
<td>Access denied because door was secured.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Interlock</td>
<td>Access Denied: Interlock</td>
<td>Denied</td>
<td>An access request was denied because the doors associated Interlock point is open.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Invalid Access Control Data Length</td>
<td>Access Denied: Invalid Access Control Data Length</td>
<td>Denied</td>
<td>The length of the retrieved data did not match the length specified in selected ACF (Access Control Format).</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Invalid Access Control Data Type</td>
<td>Access Denied: Invalid Access Control Data Type</td>
<td>Denied</td>
<td>The type of retrieved data (Wiegand/Integra) did not match the ACF (Access Control Format) type.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Invalid Smart Card Authentication</td>
<td>Access Denied: Invalid Smart Card Authentication</td>
<td>Denied</td>
<td>Failed to authenticate to the application specified by the selected SCF (Smart Card Format).</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Invalid Smart Card Data</td>
<td>Access Denied: Invalid Smart Card Data</td>
<td>Denied</td>
<td>Failed to retrieve HID application data; invalid header, invalid data length.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Invalid Smart Card Location</td>
<td>Access Denied: Invalid Smart Card Location</td>
<td>Denied</td>
<td>Application data could not be located on the card based on the selected SCF (Smart Card Format).</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Access Denied: Invalid Smart Card Type</td>
<td>Access Denied: Invalid Smart Card Type</td>
<td>Denied</td>
<td>Either the card was not found in the field or the card failed to respond to the requested RF (Radio Frequency) protocol.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: No Biometric Template</td>
<td>Access Denied: No Biometric Template</td>
<td>Denied</td>
<td>Generated when the cardholder did not have a biometric template loaded in the database, so a verification could not be done.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Denied: No Occupant Approval</td>
<td>Access Denied: No Occupant Approval</td>
<td>Denied</td>
<td>An event indicating that access was denied due to no occupant approval.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Denied: Passback</td>
<td>Access Denied: Passback</td>
<td>Denied</td>
<td>Access was denied because the credential has not exited the area before attempting to re-enter same area.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Reader Locked</td>
<td>Access Denied: Reader Locked</td>
<td>Denied</td>
<td>Generated when access was denied because the reader was locked.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Denied: Secured Mode</td>
<td>Access Denied: Secured Mode</td>
<td>Denied</td>
<td>Lock is in secured mode; no users will be allowed access.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Smart Card Format Not Found</td>
<td>Access Denied: Smart Card Format Not Found</td>
<td>Denied</td>
<td>No SCFs (Smart Card Formats) stored at the lock.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Unauthorized Arming State</td>
<td>Access Denied: Unauthorized Arming State</td>
<td>Denied</td>
<td>An access request was denied because the user was not authorized in this area when the area was armed.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Unauthorized Entry Level</td>
<td>Access Denied: Unauthorized Entry Level</td>
<td>Denied</td>
<td>An access request was denied because the user is not authorized in this area.</td>
<td></td>
</tr>
<tr>
<td>Access Denied: Unauthorized Time</td>
<td>Access Denied: Unauthorized Time</td>
<td>Denied</td>
<td>An access request was denied because the request is occurring outside the user's authorized time window(s).</td>
<td></td>
</tr>
<tr>
<td>Access Door Propped</td>
<td>Access Door Propped</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Access Door Status Monitor Shunt</td>
<td>Access Door Status Monitor Shunt</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Door Status Monitor Trouble</td>
<td>Access Door Status Monitor Trouble</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Granted</td>
<td>Access Granted</td>
<td>Granted</td>
<td>Access was granted.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Granted</td>
<td>Granted Access</td>
<td>Granted</td>
<td>Access was granted.</td>
<td></td>
</tr>
<tr>
<td>Access Granted to Destination Floor</td>
<td>Access Granted to Destination Floor</td>
<td>Granted</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access Granted - Anti-Passback Not Used</td>
<td>Granted APB Violation, No Entry Made</td>
<td>Area APB</td>
<td>Indicates that an anti-passback violation resulted and access was granted but no entry was made. This can happen when using soft anti-passback.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Granted - Anti-Passback Used</td>
<td>Granted APB Violation, Entry Made</td>
<td>Area APB</td>
<td>Indicates that an anti-passback violation resulted but access was granted and entry was made. This can happen when using soft anti-passback.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Granted - Entry Made</td>
<td>Access Granted - Entry Made</td>
<td>Granted</td>
<td>Access granted and door opened; used when latch or door sensor monitoring is present.</td>
<td></td>
</tr>
<tr>
<td>Access Granted - No Entry Made</td>
<td>Granted No Entry</td>
<td>Granted</td>
<td>Access was granted but door not opened; used when latch or door sensor monitoring is present.</td>
<td></td>
</tr>
<tr>
<td>Access Granted on Facility Code</td>
<td>Granted Facility Code</td>
<td>Granted</td>
<td>Access was granted based on a valid facility code.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Granted on Facility Code, No Entry Made</td>
<td>Granted Facility Code, No Entry</td>
<td>Granted</td>
<td>Access was granted on facility code but no entry was made at the door.</td>
<td>Yes</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Access Granted: Reader Unlocked</td>
<td>Access Granted: Reader Unlocked</td>
<td>Granted</td>
<td>Generated when access was granted because the reader was unlocked.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Granted Under Duress</td>
<td>Access Granted Under Duress</td>
<td>Duress</td>
<td>Indicates that the cardholder was granted access under duress.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Granted Under Duress - No Entry Made</td>
<td>Access Granted Under Duress - No Entry Made</td>
<td>Duress</td>
<td>Access Granted Under Duress - No Entry Made</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Level Change</td>
<td>Access Level Change</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Lockout</td>
<td>Access Lockout</td>
<td>System</td>
<td>Access denied, known code</td>
<td></td>
</tr>
<tr>
<td>Access Open</td>
<td>Access Open</td>
<td>System</td>
<td>Access for authorized users in now allowed</td>
<td></td>
</tr>
<tr>
<td>Access Point Bypass</td>
<td>Access Point Bypass</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Program Exit</td>
<td>Access Program Exit</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Relay/Trigger Fail</td>
<td>Access Relay/Trigger Fail</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Request to Exit Shunt</td>
<td>Access Request to Exit Shunt</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Schedule Change</td>
<td>Access Schedule Change</td>
<td>System</td>
<td>The access schedule has changed.</td>
<td></td>
</tr>
<tr>
<td>Access Trouble</td>
<td>Access Trouble</td>
<td>System</td>
<td>An access system trouble condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Access Zone Shunt</td>
<td>Access Zone Shunt</td>
<td>System</td>
<td>An access zone is put in the shunted state.</td>
<td></td>
</tr>
<tr>
<td>Account Status Failure</td>
<td>Account Status Failure</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Status Restore</td>
<td>Account Status Restore</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acknowledgment Action Executed</td>
<td>Acknowledgment Action Executed</td>
<td>System</td>
<td>Generated when an alarm is acknowledged and actions associated with the alarm are executed.</td>
<td></td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------------</td>
<td>------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count Incremented</td>
<td>Event Mask Count Incremented</td>
<td>Event Type</td>
<td>System</td>
<td>Description</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Alarm Mask Group Mask Count</td>
<td>Decremented</td>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Alarm Mask Group</td>
<td>Arming Failure, Active Points</td>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Alarm Monitoring Action Group</td>
<td>Executed</td>
<td>System</td>
<td>Generated when the action group is executed.</td>
<td></td>
</tr>
<tr>
<td>Alarm Monitoring Action Group</td>
<td>Failed</td>
<td>System</td>
<td>Generated when the action group execution fails.</td>
<td></td>
</tr>
<tr>
<td>Alarm Relay Disable</td>
<td>Disable</td>
<td>System</td>
<td>Generated when a device has come online or an alarm condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>Alarm Relay Disable Restored</td>
<td>Restore</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm/Restore</td>
<td>Alarm/Restore</td>
<td>System</td>
<td>Generated when a device has come online or an alarm condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>Alarm Silenced</td>
<td>Silenced</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm Tamper Loop</td>
<td>Loop</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Points Tested</td>
<td>All Points Tested</td>
<td>System</td>
<td>All points have been tested.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>All Systems Normal</td>
<td>All Systems Normal</td>
<td>Fire</td>
<td>Generated when the Notifier AM-2020 panel is booted up. This alarm may also be sent when all existing alarm conditions are resolved.</td>
<td></td>
</tr>
<tr>
<td>Analog Restore</td>
<td>Analog Restore</td>
<td>Fire</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analog Restored</td>
<td>Analog Restored</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analog Service Requested</td>
<td>Analog Service</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analog Service Required</td>
<td>Analog Service</td>
<td>Fire</td>
<td>An analog fire sensor needs to be cleaned or calibrated.</td>
<td></td>
</tr>
<tr>
<td>Anti-Passback Violation</td>
<td>Anti-Passback</td>
<td>Area Control</td>
<td>Generated when the cardholder was denied access because the entry would have violated the anti-passback rules for the area.</td>
<td>Yes</td>
</tr>
<tr>
<td>Archive Server Failure</td>
<td>Archive Server</td>
<td>Video</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Archive Server Failure Archive Location Full</td>
<td>Archive Server Failure</td>
<td>Video</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>ARDIS Module Communication Loss</td>
<td>ARDIS Module Communication Loss</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARDIS Module Communication Restored</td>
<td>ARDIS Module Communication Restored</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area Closed</td>
<td>Area Closed</td>
<td>Area Control</td>
<td>Generated when access was denied because the area being entered is closed.</td>
<td>Yes</td>
</tr>
<tr>
<td>Area Limit Exceeded</td>
<td>Area Limit Exceeded</td>
<td>Area Control</td>
<td>Generated when access was denied because the area limit would have been exceeded.</td>
<td>Yes</td>
</tr>
<tr>
<td>Area Watch End</td>
<td>Area Watch End</td>
<td>System</td>
<td>Area watch feature has been deactivated</td>
<td></td>
</tr>
<tr>
<td>Area Watch Start</td>
<td>Area Watch Start</td>
<td>System</td>
<td>Area watch feature has been activated</td>
<td></td>
</tr>
<tr>
<td>Arm/Disarm Command Accepted</td>
<td></td>
<td></td>
<td>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”</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Arm/Disarm Command Denied</td>
<td>Arm/Disarm Command Denied</td>
<td>System</td>
<td>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”.</td>
<td></td>
</tr>
<tr>
<td>Armed Perimeter Delay</td>
<td>Armed Perimeter Delay</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Armed Perimeter Instant</td>
<td>Armed Perimeter Instant</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Armed Stay</td>
<td>Armed Stay</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Denied - Invalid Access</td>
<td>Asset Denied - Invalid Access</td>
<td>Asset</td>
<td>Generated when the asset was denied because the cardholder had invalid access levels.</td>
<td>Yes</td>
</tr>
<tr>
<td>Asset Denied - Invalid Asset</td>
<td>Asset Denied - Invalid Asset</td>
<td>Asset</td>
<td>Generated when the asset was denied because of an invalid asset (the asset was not found in the controller).</td>
<td>Yes</td>
</tr>
<tr>
<td>Asset Denied - Invalid Cardholder</td>
<td>Asset Denied - Invalid Cardholder</td>
<td>Asset</td>
<td>Generated when the asset was denied because of an invalid cardholder.</td>
<td>Yes</td>
</tr>
<tr>
<td>Asset Denied - No Asset Privileges</td>
<td>Asset Denied - No Asset Privileges</td>
<td>Asset</td>
<td>Generated when the asset was denied because the cardholder had no asset privileges.</td>
<td></td>
</tr>
<tr>
<td>Asset Granted - Asset Owner</td>
<td>Asset Granted - Asset Owner</td>
<td>Asset</td>
<td>Generated when the asset was granted because the cardholder was the asset owner.</td>
<td>Yes</td>
</tr>
<tr>
<td>Asset Granted - Asset Privileges Only</td>
<td>Asset Granted - Asset Privileges Only</td>
<td>Asset</td>
<td>Generated when the asset was granted because the cardholder had asset privileges.</td>
<td>Yes</td>
</tr>
<tr>
<td>Audible Alarm</td>
<td>Audible Alarm</td>
<td>Trouble</td>
<td>An audible alarm condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Audible Alarm Restore</td>
<td>Audible Alarm Restore</td>
<td>Trouble</td>
<td>An audible alarm condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>Audibles Silenced</td>
<td>Audibles Silenced</td>
<td>Fire</td>
<td>Generated when all the alarm bells have been turned off on the controller.</td>
<td></td>
</tr>
<tr>
<td>Audibles Unsilenced</td>
<td>Audibles Unsilenced</td>
<td>Fire</td>
<td>Generated when all the alarm bells have been turned back on for the controller.</td>
<td></td>
</tr>
<tr>
<td>Audit Trail Cleared</td>
<td>Audit Trail Cleared</td>
<td>System</td>
<td>Generated when the audit (event) log is cleared.</td>
<td></td>
</tr>
<tr>
<td>Audit Trail Limit Reached</td>
<td>Audit Trail Limit Reached</td>
<td>System</td>
<td>Informs OnGuard the audit (event) log is becoming full and will be overwritten.</td>
<td></td>
</tr>
<tr>
<td>Auto Arming Time Changed</td>
<td>Auto Arming Time Changed</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-Arm Failed</td>
<td>Auto-Arm Failed</td>
<td>Trouble</td>
<td>An automatic arm has failed.</td>
<td></td>
</tr>
<tr>
<td>Automatic Closing</td>
<td>Automatic Closing</td>
<td>Open/Close</td>
<td>The system was armed automatically.</td>
<td></td>
</tr>
<tr>
<td>Automatic Opening</td>
<td>Automatic Opening</td>
<td>Open/Close</td>
<td>The system has disarmed automatically.</td>
<td></td>
</tr>
<tr>
<td>Automatic Phone Test</td>
<td>Automatic Phone Test</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic Test</td>
<td>Automatic Test</td>
<td>System</td>
<td>Automatic communication test report</td>
<td></td>
</tr>
<tr>
<td>Auxiliary Power Fault</td>
<td>Auxiliary Power Fault</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auxiliary Power Supply AC Loss</td>
<td>Auxiliary Power Supply AC Loss</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auxiliary Power Supply AC Restored</td>
<td>Auxiliary Power Supply AC Restored</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auxiliary Power Supply Communication Loss</td>
<td>Auxiliary Power Supply Communication Loss</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Auxiliary Power Supply</td>
<td>Auxiliary Power Supply</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Communication Restored</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auxiliary Power Supply</td>
<td>Auxiliary Power Supply</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Fault</td>
<td>Fault</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restored</td>
<td>Restored</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auxiliary Power Supply</td>
<td>Auxiliary Power Supply</td>
<td>Trouble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Output Low</td>
<td>Output Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restored</td>
<td>Restored</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Map Found</td>
<td>Background Map Found</td>
<td>Video</td>
<td>Generated when background stickers are detected.</td>
<td></td>
</tr>
<tr>
<td>Background Map Not Found</td>
<td>Background Map Not Found</td>
<td>Video</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Background Scene Changed</td>
<td>Background Scene Changed</td>
<td>Video</td>
<td>Indicates that part of the background has changed. This can be from something added to the scene or something removed from the scene.</td>
<td></td>
</tr>
<tr>
<td>Background Scene Change</td>
<td>Change</td>
<td>Video</td>
<td>The alarm is restored.</td>
<td></td>
</tr>
<tr>
<td>Change Restored</td>
<td>Restored</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bad 9112 Packet</td>
<td>Bad 9112 Packet</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Battery Test Fail</td>
<td>Battery Test Fail</td>
<td>System</td>
<td>A battery test fail condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Battery Test Fail Restore</td>
<td>Battery Test Fail Restore</td>
<td>System</td>
<td>A battery test fail condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>Bell # Disable</td>
<td>Bell # Disable</td>
<td>Relay/Sounder</td>
<td>Bell # has been disabled.</td>
<td></td>
</tr>
<tr>
<td>Bell # Disable Restore</td>
<td>Bell # Disable Restore</td>
<td>Relay/Sounder</td>
<td>Bell # has been restored.</td>
<td></td>
</tr>
<tr>
<td>Bell Fault</td>
<td>Bell Fault</td>
<td>Relay/Sounder</td>
<td>A trouble condition has been detected on a local bell, siren, or annunciator.</td>
<td></td>
</tr>
<tr>
<td>Bell Restore</td>
<td>Bell Restore</td>
<td>Relay/Sounder</td>
<td>A trouble condition has been restored on a local bell, siren, or annunciator.</td>
<td></td>
</tr>
<tr>
<td>Biometric Mismatch</td>
<td>Biometric Mismatch</td>
<td>Denied</td>
<td>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.</td>
<td>Yes</td>
</tr>
<tr>
<td>Biometric Verify Mode Disabled</td>
<td>Biometric Verify Mode Disabled</td>
<td>System</td>
<td>Generated when biometric verify mode is disabled.</td>
<td></td>
</tr>
<tr>
<td>Biometric Verify Mode Enabled</td>
<td>Biometric Verify Mode Enabled</td>
<td>System</td>
<td>Generated when biometric verify mode is enabled.</td>
<td></td>
</tr>
<tr>
<td>Blind Camera (AI)</td>
<td>Blind Camera (AI)</td>
<td>Video</td>
<td>Indicates that level of camera blindness (covered by some sort of obstacle) exceeded configured threshold.</td>
<td></td>
</tr>
<tr>
<td>Blind Camera (AI) Restored</td>
<td>Blind Camera (AI) Restored</td>
<td>Video</td>
<td>The alarm is restored.</td>
<td></td>
</tr>
<tr>
<td>Block Acknowledge</td>
<td>Block Acknowledge</td>
<td>Fire</td>
<td>Generated when a block acknowledge command is sent. This command acknowledges any existing unacknowledged alarms in the system all at once.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Brightness Change</td>
<td>Brightness Change</td>
<td>Video</td>
<td>Generated when a change in overall brightness level of the scene is detected.</td>
<td></td>
</tr>
<tr>
<td>Brightness Change</td>
<td>Brightness Change</td>
<td>Video</td>
<td>Generated when changes in brightness level are no longer exceeding the user defined threshold.</td>
<td></td>
</tr>
<tr>
<td>Brightness Change</td>
<td>Brightness Change</td>
<td>Video</td>
<td>Generated when changes in brightness level are no longer exceeding the user defined threshold.</td>
<td></td>
</tr>
<tr>
<td>Burglary Alarm</td>
<td>Burglary Alarm</td>
<td>Burglary</td>
<td>A burglary alarm condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Burglary Alert</td>
<td>Burglary Alert</td>
<td>Burglary</td>
<td>A burglary alarm condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>Burglary Bypass</td>
<td>Burglary Bypass</td>
<td>Burglary</td>
<td>A burglary zone has been bypassed.</td>
<td></td>
</tr>
<tr>
<td>Burglary Cancel</td>
<td>Burglary Cancel</td>
<td>Burglary</td>
<td>A burglary zone has been cancelled by an authorized user.</td>
<td></td>
</tr>
<tr>
<td>Burglary Close</td>
<td>Burglary Close</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Burglary Inactive</td>
<td>Burglary Inactive</td>
<td>Burglary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Burglary Open</td>
<td>Burglary Open</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Burglary Restore</td>
<td>Burglary Restore</td>
<td>Burglary</td>
<td>A burglary alarm/trouble condition has been eliminated.</td>
<td></td>
</tr>
<tr>
<td>Burglary Supervisory</td>
<td>Burglary Supervisory</td>
<td>Burglary</td>
<td>An unsafe intrusion detection system condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Burglary Test</td>
<td>Burglary Test</td>
<td>Burglary</td>
<td>A burglary zone has been activated during testing.</td>
<td></td>
</tr>
<tr>
<td>Burglary Trouble</td>
<td>Burglary Trouble</td>
<td>Burglary</td>
<td>A burglary trouble condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Burglary Trouble</td>
<td>Burglary Trouble</td>
<td>Burglary</td>
<td>A burglary trouble condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Burglary Trouble</td>
<td>Burglary Trouble</td>
<td>Burglary</td>
<td>A burglary trouble condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Burglary Trouble</td>
<td>Burglary Trouble</td>
<td>Burglary</td>
<td>A burglary trouble condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Burglary Trouble</td>
<td>Burglary Trouble</td>
<td>Burglary</td>
<td>A burglary trouble condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------</td>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Burglary Unbypass</td>
<td>Burglary Unbypass</td>
<td>Burglary</td>
<td>Burglary zone bypass has been removed.</td>
<td></td>
</tr>
<tr>
<td>Burglary Verified</td>
<td>Burglary Verified</td>
<td>Burglary</td>
<td>A burglary alarm has occurred and been verified within programmed conditions.</td>
<td></td>
</tr>
<tr>
<td>Busy Seconds</td>
<td>Busy Seconds</td>
<td>System</td>
<td>The percent of time the receiver’s line card is online.</td>
<td></td>
</tr>
<tr>
<td>Bypass - Closed</td>
<td>Bypass - Closed</td>
<td>Open/ Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bypass Restore</td>
<td>Bypass Restore</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Battery Low</td>
<td>C900 Battery Low</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Battery Restore</td>
<td>C900 Battery Restore</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Input Open</td>
<td>C900 Input Open</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Input Restored</td>
<td>C900 Input Restored</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Input Shorted</td>
<td>C900 Input Shorted</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Intercepted</td>
<td>C900 Intercepted</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Intercepted</td>
<td>C900 Intercepted</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Output Activated</td>
<td>C900 Output Activated</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Output Deactivated</td>
<td>C900 Output Deactivated</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Reboot</td>
<td>C900 Reboot</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Switched to Fallback</td>
<td>C900 Switched to Fallback</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C900 Switched to Intercept</td>
<td>C900 Switched to Intercept</td>
<td>C900</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cabinet Tamper Active</td>
<td>Cabinet Tamper</td>
<td>System</td>
<td>Generated when a cabinet tamper condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Cabinet Tamper Restored</td>
<td>Cancelled Cabinet Tamper</td>
<td>System</td>
<td>Generated when a cabinet tamper condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>Callback Request</td>
<td>Callback Request</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Callback Request</td>
<td>Call Conferenced</td>
<td>Intercom</td>
<td>Generated when an intercom call has been conferenced.</td>
<td></td>
</tr>
<tr>
<td>Call Disconnected</td>
<td>Call Disconnected</td>
<td>Intercom</td>
<td>Generated when an intercom call has been disconnected.</td>
<td></td>
</tr>
<tr>
<td>Call Ended</td>
<td>Call Ended</td>
<td>Intercom</td>
<td>Generated when a call has ended.</td>
<td></td>
</tr>
<tr>
<td>Call Established</td>
<td>Call Established</td>
<td>Intercom</td>
<td>Generated when an intercom call is answered.</td>
<td></td>
</tr>
<tr>
<td>Call Failed</td>
<td>Call Failed</td>
<td>Intercom</td>
<td>Generated when an intercom call fails.</td>
<td></td>
</tr>
<tr>
<td>Call to a busy subscriber</td>
<td>Call to a busy subscriber</td>
<td>Intercom</td>
<td>Generated when an intercom call has been placed to a busy subscriber.</td>
<td></td>
</tr>
<tr>
<td>Call to an open subscriber</td>
<td>Call to an open subscriber</td>
<td>Intercom</td>
<td>Generated when an intercom call has been placed to an open subscriber.</td>
<td></td>
</tr>
<tr>
<td>Call to a private subscriber</td>
<td>Call to a private subscriber</td>
<td>Intercom</td>
<td>Generated when a call has been placed to a private subscriber.</td>
<td></td>
</tr>
<tr>
<td>Call Transferred</td>
<td>Call Transferred</td>
<td>Intercom</td>
<td>Generated when a call was transferred.</td>
<td></td>
</tr>
<tr>
<td>Camera Enabled</td>
<td>Camera Enabled</td>
<td>NetDVMS</td>
<td>The camera is enabled in the NetDVMS Administrator.</td>
<td></td>
</tr>
<tr>
<td>Camera Disabled</td>
<td>Camera Disabled</td>
<td>NetDVMS</td>
<td>The camera is disabled in the NetDVMS Administrator.</td>
<td></td>
</tr>
<tr>
<td>Camera Motion</td>
<td>Camera Motion</td>
<td>NetDVMS</td>
<td>Generated when motion has been detected on a given input channel (camera).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Motion is considered any change in the environment within the field of view</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>of the camera. Sensitivity is determined by the motion detection settings in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the NetDVMS Administrator.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Camera Tamper Active</td>
<td>Camera Tamper Active</td>
<td>Video</td>
<td>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.)</td>
<td></td>
</tr>
<tr>
<td>Camera Tamper Restored</td>
<td>Camera Tamper Restored</td>
<td>Video</td>
<td>The alarm is restored. LNVR changed camera settings back to normal.</td>
<td></td>
</tr>
<tr>
<td>Cancel Alarm</td>
<td>Cancel Alarm</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cancel Entire Sale</td>
<td>Cancel Entire Sale</td>
<td>POS</td>
<td>Generated when a transaction is used to indicate that an entire sale was cancelled.</td>
<td></td>
</tr>
<tr>
<td>Cannot Open Door: Interlock Area Busy</td>
<td>Cannot Open Door: Interlock Area Busy</td>
<td>Area Control</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Capture Source Mismatch</td>
<td>Capture Source Mismatch</td>
<td>Video</td>
<td>Indicates that user-specified IP Camera type in OnGuard does not match actual IP Camera type.</td>
<td></td>
</tr>
<tr>
<td>Carbon Monoxide Detected</td>
<td>Carbon Monoxide Detected</td>
<td>Gas</td>
<td>Generated when carbon monoxide has been detected by an alarm.</td>
<td></td>
</tr>
<tr>
<td>Card Added</td>
<td>Card Added</td>
<td>System</td>
<td>Generated when a card has been added.</td>
<td></td>
</tr>
<tr>
<td>Card Assigned</td>
<td>Card Assigned</td>
<td>System</td>
<td>An access ID has been added to the controller.</td>
<td></td>
</tr>
<tr>
<td>Card Deleted</td>
<td>Card Deleted</td>
<td>System</td>
<td>An access ID has been deleted from the controller.</td>
<td></td>
</tr>
<tr>
<td>Card Only Mode Denied: Blocked Mode</td>
<td>Card Only Mode Denied: Blocked Mode</td>
<td>System</td>
<td>Automatic scheduled change to card only mode was denied because lock is in blocked mode.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Card Only Mode Denied: Secured Mode</td>
<td>Card Only Mode Denied: Secured Mode</td>
<td>System</td>
<td>Automatic scheduled change to card only mode was denied because lock is in secured mode.</td>
<td></td>
</tr>
<tr>
<td>Cash Amount Tendered</td>
<td>Cash Amount Tendered</td>
<td>POS</td>
<td>Generated when an event is used to indicate that a cash amount has been tendered.</td>
<td></td>
</tr>
<tr>
<td>Cash or Safe Drop</td>
<td>Cash or Safe Drop</td>
<td>POS</td>
<td>Generated when a transaction indicating a cash or safe drop has occurred.</td>
<td></td>
</tr>
<tr>
<td>Change Due</td>
<td>Change Due</td>
<td>POS</td>
<td>Generated when a transaction indicating the change due has occurred.</td>
<td></td>
</tr>
<tr>
<td>Change of State</td>
<td>Change of State</td>
<td>System</td>
<td>An expansion/peripheral device is reporting a new condition or state change.</td>
<td></td>
</tr>
<tr>
<td>Charge Account Tender</td>
<td>Charge Account Tender</td>
<td>POS</td>
<td>Generated when a charge account was used as tender.</td>
<td></td>
</tr>
<tr>
<td>Check Tender</td>
<td>Check Tender</td>
<td>POS</td>
<td>Generated when a check was used as tender.</td>
<td></td>
</tr>
<tr>
<td>Checksum Fail</td>
<td>Checksum Fail</td>
<td>System</td>
<td>A checksum failure has been detected.</td>
<td></td>
</tr>
<tr>
<td>Cipher Mode Disabled</td>
<td>Cipher Mode Disabled</td>
<td>System</td>
<td>Generated when Cipher mode is disabled for a reader.</td>
<td></td>
</tr>
<tr>
<td>Cipher Mode Enabled</td>
<td>Cipher Mode Enabled</td>
<td>System</td>
<td>Generated when cipher mode is enabled for a reader. When this occurs card data can be entered via the keypad.</td>
<td></td>
</tr>
<tr>
<td>Clerk Name or Number</td>
<td>Clerk Name or Number</td>
<td>POS</td>
<td>A transaction that reports the clerk's name or number.</td>
<td></td>
</tr>
<tr>
<td>Close Area</td>
<td>Close Area</td>
<td>Open/Close</td>
<td>The system has been partially armed</td>
<td></td>
</tr>
<tr>
<td>Close by User</td>
<td>Close by User</td>
<td>Open/Close</td>
<td>The area has been armed by a user.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Close Exception</td>
<td>Close Exception</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Close Out of Window</td>
<td>Close Out of Window</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Closing</td>
<td>Closing</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Closing Delinquent</td>
<td>Closing Delinquent</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Closing Extend</td>
<td>Closing Extend</td>
<td>Open/Close</td>
<td>The closing time has been extended.</td>
<td></td>
</tr>
<tr>
<td>Closing Out of Window by User</td>
<td>Closing Out of Window by User</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Closing Report</td>
<td>Closing Report</td>
<td>Open/Close</td>
<td>The system is armed and normal</td>
<td></td>
</tr>
<tr>
<td>Closing Switch</td>
<td>Closing Switch</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Closing Time Changed</td>
<td>Closing Time Changed</td>
<td>Open/Close</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Combustion Alarm</td>
<td>Combustion Alarm</td>
<td>Open/Close</td>
<td>A combustion alarm condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Combustion Alarm Restore</td>
<td>Combustion Alarm Restore</td>
<td>Open/Close</td>
<td>A combustion alarm condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>Command (#) Set From Reader</td>
<td>Command (#) Set From Reader</td>
<td>System</td>
<td>Generated when the reader keypad command &quot;(#)&quot;) was executed.</td>
<td></td>
</tr>
<tr>
<td>Command Pin +10 Set From Reader</td>
<td>Command Pin +10 Set From Reader</td>
<td>System</td>
<td>Indicates the reader command &quot;Pin +10&quot; was executed.</td>
<td></td>
</tr>
<tr>
<td>Command Pin +20 Set From Reader</td>
<td>Command Pin +20 Set From Reader</td>
<td>System</td>
<td>Indicates the reader command &quot;Pin +20&quot; was executed.</td>
<td></td>
</tr>
<tr>
<td>Command Sent</td>
<td>Command Sent</td>
<td>System</td>
<td>A command has been sent to an expansion/peripheral device.</td>
<td></td>
</tr>
<tr>
<td>Communication Access Denied</td>
<td>Communication Access Denied</td>
<td>System</td>
<td>Indicates that a wrong password has been entered while logging on to a communication device.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Communication Initialization Failed</td>
<td>Communication Initialization Failed</td>
<td>System</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Communication Trouble Restore</td>
<td>Communication Trouble Restore</td>
<td>System</td>
<td>A communication trouble has been restored.</td>
<td></td>
</tr>
<tr>
<td>Communications Fail</td>
<td>Communications Fail</td>
<td>System</td>
<td>A communication has failed.</td>
<td></td>
</tr>
<tr>
<td>Communications Lost</td>
<td>Communications Lost</td>
<td>System</td>
<td>Generated when communications to the device have been lost.</td>
<td></td>
</tr>
<tr>
<td>Communications Lost - Primary Path</td>
<td>Primary Communication Path Lost</td>
<td>System</td>
<td>Generated when the primary path lost communication with the host.</td>
<td></td>
</tr>
<tr>
<td>Communications Lost - Secondary Path</td>
<td>Secondary Communication Path Lost</td>
<td>System</td>
<td>Generated when the secondary path loses communication with the host.</td>
<td></td>
</tr>
<tr>
<td>Communications Path Switched - Primary to Secondary</td>
<td>Communications Path Switched - Primary to Secondary</td>
<td>System</td>
<td>Generated when the communication path has been switched from the primary path to the secondary path.</td>
<td></td>
</tr>
<tr>
<td>Communications Path Switched Secondary to Primary</td>
<td>Communications Path Switched Secondary to Primary</td>
<td>System</td>
<td>Generated when the communication path has switched from the secondary path to the primary path.</td>
<td></td>
</tr>
<tr>
<td>Communications Restore</td>
<td>Communications Restore</td>
<td>System</td>
<td>Generated when communications have been restored.</td>
<td></td>
</tr>
<tr>
<td>Communications Restored</td>
<td>Communications Restored</td>
<td>System</td>
<td>Generated when communications to the device have been restored.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Communications Restored - Primary Path</td>
<td>Primary Communication Path Restored</td>
<td>System</td>
<td>Generated when the primary path restored communication with the host.</td>
<td></td>
</tr>
<tr>
<td>Communications Restored - Secondary Path</td>
<td>Secondary Communication Path Restored</td>
<td>System</td>
<td>Generated when the secondary path restored communication with the host.</td>
<td></td>
</tr>
<tr>
<td>Communications Trouble</td>
<td>Communications Trouble</td>
<td>System</td>
<td>A communications trouble has been detected.</td>
<td></td>
</tr>
<tr>
<td>Communications With Host Lost</td>
<td>Communications With Host Lost</td>
<td>System</td>
<td>An event was generated by the hardware when communications with the host was lost.</td>
<td></td>
</tr>
<tr>
<td>Communications With Host Restored</td>
<td>Communications With Host Restored</td>
<td>System</td>
<td>An event was generated by the hardware when communications with the host was restored.</td>
<td></td>
</tr>
<tr>
<td>Complimentary Tender</td>
<td>Complimentary Tender</td>
<td>POS</td>
<td>Generated when the tender was complimentary.</td>
<td></td>
</tr>
<tr>
<td>Computer Trouble</td>
<td>Computer Trouble</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conferenced Call</td>
<td>Intercom</td>
<td></td>
<td>Generated if a call is conferenced together with another call.</td>
<td></td>
</tr>
<tr>
<td>Congestion</td>
<td>Congestion</td>
<td>Video</td>
<td>Generated when the user-specified level and pattern of congestion is detected within a region of interest.</td>
<td></td>
</tr>
<tr>
<td>Congestion Restored</td>
<td>Congestion Restored</td>
<td>Video</td>
<td>Generated 8 seconds after last detection of a Congestion event.</td>
<td></td>
</tr>
<tr>
<td>Controller Connection Mismatch</td>
<td>Controller Connection Mismatch</td>
<td>System</td>
<td>Generated when the OnGuard attempts to make a connection to a controller by upgrading or degrading the connection while the controller is online.</td>
<td></td>
</tr>
</tbody>
</table>
### Alarm Monitoring User Guide

#### Controller Encryption Error

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 plain connection, and then the DIR switch 8 is turned on. |

#### CPU Data Error

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>A CPU data error was detected.</td>
</tr>
</tbody>
</table>

#### CPU Utilization Threshold Exceeded

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Generated by an LNVR recorder when current CPU level exceeds the user defined limit.</td>
</tr>
</tbody>
</table>

#### CPU Utilization Threshold Restored

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Generated by an LNVR recorder when the current CPU level drop below the user defined limit.</td>
</tr>
</tbody>
</table>

#### Credit Card Tendered

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS</td>
<td>Generated when a credit card was used as tender.</td>
</tr>
</tbody>
</table>

#### Cross Zone Trouble

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trouble</td>
<td>An event that reports the current time.</td>
</tr>
</tbody>
</table>

#### Current Time

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS</td>
<td>An event that reports the current time.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Database Error Event Polling Stopped</td>
<td>Database Error Event Polling Stopped</td>
</tr>
<tr>
<td>Database Error in Panel Download</td>
<td>Database Error in Panel Download</td>
</tr>
<tr>
<td>Data Lost</td>
<td>Data Lost</td>
</tr>
<tr>
<td>Date Changed</td>
<td>Date Changed</td>
</tr>
<tr>
<td>Day Trouble</td>
<td>Day Trouble</td>
</tr>
<tr>
<td>Day Trouble Restore</td>
<td>Day Trouble Restore</td>
</tr>
<tr>
<td>Day/Night Alarm</td>
<td>Day/Night Alarm</td>
</tr>
<tr>
<td>Day/Night Alarm Restore</td>
<td>Day/Night Alarm Restore</td>
</tr>
<tr>
<td>Daylight Saving Time Audit</td>
<td>Daylight Saving Time Audit</td>
</tr>
<tr>
<td>Deactivate Output</td>
<td>Deactivate Output</td>
</tr>
<tr>
<td>Dealer ID</td>
<td>Dealer ID</td>
</tr>
<tr>
<td>Debit, ATM, Check Card Tender</td>
<td>Debit, ATM, Check Card Tender</td>
</tr>
<tr>
<td>Deferred Close</td>
<td>Deferred Close</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Deferred Open/Close</td>
<td>Deferred Open/Close</td>
</tr>
<tr>
<td>Denied, Badge Not in Panel</td>
<td>Denied, Badge Not in Panel</td>
</tr>
<tr>
<td>Denied Count Exceeded</td>
<td>Denied Count Exceeded</td>
</tr>
<tr>
<td>Denied Low Battery</td>
<td>Denied Low Battery</td>
</tr>
<tr>
<td>Denied, No Command Authority</td>
<td>Denied, No Command Authority</td>
</tr>
<tr>
<td>Denied - No Host Approval</td>
<td>Denied - No Host Approval</td>
</tr>
<tr>
<td>Denied, Not Authorized</td>
<td>Denied, Not Authorized</td>
</tr>
<tr>
<td>Denied, PIN Only Request</td>
<td>Denied, PIN Only Request</td>
</tr>
<tr>
<td>Denied - Unauthorized Assets</td>
<td>Denied - Unauthorized Assets</td>
</tr>
<tr>
<td>Denied Under Duress</td>
<td>Access Denied Under Duress</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Denied Unmask, Active Zones in Group</td>
<td>Denied Unmask - Active Zones in Group</td>
</tr>
<tr>
<td>Deny Count Exceeded</td>
<td>Deny Count Exceeded</td>
</tr>
<tr>
<td>Deposit Amount Paid Pending Purchase</td>
<td>Deposit Amount Paid Pending Purchase</td>
</tr>
<tr>
<td>Deposit Return</td>
<td>Deposit Return</td>
</tr>
<tr>
<td>Detector High Sensitivity</td>
<td>Detector High Sensitivity</td>
</tr>
<tr>
<td>Detector High Sensitivity Restore</td>
<td>Detector High Sensitivity Restore</td>
</tr>
<tr>
<td>Detector Low Sensitivity</td>
<td>Detector Low Sensitivity</td>
</tr>
<tr>
<td>Detector Low Sensitivity Restore</td>
<td>Detector Low Sensitivity Restore</td>
</tr>
<tr>
<td>Detector Test</td>
<td>Detector Test</td>
</tr>
<tr>
<td>Detector Test Fail</td>
<td>Detector Test Fail</td>
</tr>
<tr>
<td>Detector Test OK</td>
<td>Detector Test OK</td>
</tr>
<tr>
<td>Device Turned Off</td>
<td>Device Turned Off</td>
</tr>
<tr>
<td>Device Turned On</td>
<td>Device Turned On</td>
</tr>
<tr>
<td>Device Type Mismatch</td>
<td>Device Type Mismatch</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Diagnostic</td>
</tr>
<tr>
<td>Diagnostic Error</td>
<td>Diagnostic Error</td>
</tr>
<tr>
<td>Dial Out Method</td>
<td>Dial Out Method</td>
</tr>
<tr>
<td>Dialer Disabled</td>
<td>Dialer Disabled</td>
</tr>
<tr>
<td>Dialer Disabled Restore</td>
<td>Dialer Disabled Restore</td>
</tr>
<tr>
<td>Dialer Shutdown</td>
<td>Dialer Shutdown</td>
</tr>
<tr>
<td>Dialing Error</td>
<td>Dialing Error</td>
</tr>
<tr>
<td>Dialup Last Connection Time Expired</td>
<td>Dialup Last Connection Time Expired</td>
</tr>
<tr>
<td>Dialup Stored Command Limit Exceeded</td>
<td>Dialup Stored Command Limit Exceeded</td>
</tr>
<tr>
<td>Disable Intercept Mode</td>
<td>Disable Intercept Mode</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Directional Motion</td>
<td>Directional Motion</td>
</tr>
<tr>
<td>Directional Motion Restored</td>
<td>Directional Motion Restored</td>
</tr>
<tr>
<td>Disarm From Alarm</td>
<td>Disarm From Alarm</td>
</tr>
<tr>
<td>Discount Entered as Absolute Amount</td>
<td>Discount Entered as Absolute Amount</td>
</tr>
<tr>
<td>Discount Entered as Percentage</td>
<td>Discount Entered as Percentage</td>
</tr>
<tr>
<td>Disk Read Utilization Threshold Exceeded</td>
<td>Disk Read Utilization Threshold Exceeded</td>
</tr>
<tr>
<td>Disk Read Utilization Threshold Restored</td>
<td>Disk Read Utilization Threshold Restored</td>
</tr>
<tr>
<td>Disk Write Utilization Threshold Exceeded</td>
<td>Disk Write Utilization Threshold Exceeded</td>
</tr>
<tr>
<td>Disk Write Utilization Threshold Restored</td>
<td>Disk Write Utilization Threshold Restored</td>
</tr>
<tr>
<td>Door Close</td>
<td>Door Close</td>
</tr>
<tr>
<td>Door Contact Tamper Active</td>
<td>Door Contact Tamper</td>
</tr>
<tr>
<td>Door Contact Tamper Restored</td>
<td>Door Contact Tamper Cancelled</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Door Cycled</td>
<td>Door Cycled</td>
</tr>
<tr>
<td>Door Forced</td>
<td>Door Forced</td>
</tr>
<tr>
<td>Door Forced Open</td>
<td>Door Forced Open</td>
</tr>
<tr>
<td>Door Forced Open Masked</td>
<td>Door Forced Open Masked</td>
</tr>
<tr>
<td>Door Forced Open Restored</td>
<td>Door Forced Open Cancelled</td>
</tr>
<tr>
<td>Door Forced Open Unmasked</td>
<td>Door Forced Open Unmasked</td>
</tr>
<tr>
<td>Door Forced Trouble</td>
<td>Door Forced Trouble</td>
</tr>
<tr>
<td>Door Held Open</td>
<td>Door Held Open</td>
</tr>
<tr>
<td>Door Held Open Masked</td>
<td>Door Held Open Masked</td>
</tr>
<tr>
<td>Door Held Open Restored</td>
<td>Door Held Open Cancelled</td>
</tr>
<tr>
<td>Door Held Open Unmasked</td>
<td>Door Held Open Unmasked</td>
</tr>
<tr>
<td>Door Left Open</td>
<td>Door Left Open</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Door Left Open Alarm</td>
<td>Door Left Open Alarm</td>
</tr>
<tr>
<td>Door Left Open Restore</td>
<td>Door Left Open Restore</td>
</tr>
<tr>
<td>Door Left Open Trouble</td>
<td>Door Left Open Trouble</td>
</tr>
<tr>
<td>Door Locked</td>
<td>Door Locked</td>
</tr>
<tr>
<td>Door Open</td>
<td>Door Open</td>
</tr>
<tr>
<td>Door Open From Inside</td>
<td>Door Open From Inside</td>
</tr>
<tr>
<td>Door Request</td>
<td>Door Request</td>
</tr>
<tr>
<td>Door Restore</td>
<td>Door Restore</td>
</tr>
<tr>
<td>Door Secured</td>
<td>Door Secured</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Door Shunt Command Executed From Reader</td>
<td>Door Shunt Command Executed From Reader</td>
</tr>
<tr>
<td>Door Shunt Command Results - Cancelled</td>
<td>Door Shunt Command Results - Cancelled</td>
</tr>
<tr>
<td>Door Station</td>
<td>Door Station</td>
</tr>
<tr>
<td>Door Unlocked</td>
<td>Door Unlocked</td>
</tr>
<tr>
<td>Drift Compensation Error</td>
<td>Drift Compensation Error</td>
</tr>
<tr>
<td>Driver Error in Panel Download</td>
<td>Driver Error in Panel Download</td>
</tr>
<tr>
<td>Duct Alarm</td>
<td>Duct Alarm</td>
</tr>
<tr>
<td>Duct Alarm Restore</td>
<td>Duct Alarm Restore</td>
</tr>
<tr>
<td>Duress Access Grant</td>
<td>Duress Access Grant</td>
</tr>
<tr>
<td>Duress Egress Grant</td>
<td>Duress Egress Grant</td>
</tr>
<tr>
<td>DURESS - Interlock Area Busy</td>
<td>DURESS - Interlock Area Busy</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Egress Denied</td>
<td>Egress</td>
</tr>
<tr>
<td>Egress Granted</td>
<td>Egress</td>
</tr>
<tr>
<td>Elevator Terminal Mode Access to Authorized Floors</td>
<td>Elevator Terminal Mode Access to Authorized Floors</td>
</tr>
<tr>
<td>Elevator Terminal Mode Default Floor</td>
<td>Elevator Terminal Mode Default Floor</td>
</tr>
<tr>
<td>Elevator Terminal Mode Default Floor or User Entry of Destination Floor</td>
<td>Elevator Terminal Mode Default Floor or User Entry of Destination Floor</td>
</tr>
<tr>
<td>Elevator Terminal Mode User Entry of Destination Floor</td>
<td>Elevator Terminal Mode User Entry of Destination Floor</td>
</tr>
<tr>
<td>Embedded Analytics Failure</td>
<td>Embedded Analytics Failure</td>
</tr>
<tr>
<td>Embedded Analytics Restored</td>
<td>Embedded Analytics Restored</td>
</tr>
<tr>
<td>Employee Sign Off</td>
<td>Employee Sign Off</td>
</tr>
<tr>
<td>Employee Sign On</td>
<td>Employee Sign On</td>
</tr>
<tr>
<td>Exit Request Denied: Interlock Area Busy</td>
<td>Exit Request Denied: Interlock Area Busy</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Extended Held Command Denied</td>
<td>Extended Held Command Denied</td>
</tr>
<tr>
<td>Extended Held Command Set From Reader</td>
<td>Extended Held Command Set From Reader</td>
</tr>
<tr>
<td>Extended Held Open Mode Disabled</td>
<td>Extended Held Open Mode Disabled</td>
</tr>
<tr>
<td>Extended Held Open Mode Enabled</td>
<td>Extended Held Open Mode Enabled</td>
</tr>
<tr>
<td>Facial Detection</td>
<td>Facial Detection</td>
</tr>
<tr>
<td>Facial Detection Restored</td>
<td>Facial Detection Restored</td>
</tr>
<tr>
<td>Facility Code Only Mode Denied: Blocked Mode</td>
<td>Facility Code Only Mode Denied: Blocked Mode</td>
</tr>
<tr>
<td>Facility Code Only Mode Denied: Secured Mode</td>
<td>Facility Code Only Mode Denied: Secured Mode</td>
</tr>
<tr>
<td>Facility Occupancy Too Low</td>
<td>Facility Occupancy Too Low</td>
</tr>
<tr>
<td>Facility Occupancy Too Low Restored</td>
<td>Facility Occupancy Too Low Restored</td>
</tr>
<tr>
<td>Facility Occupancy Too High</td>
<td>Facility Occupancy Too High</td>
</tr>
<tr>
<td>Facility Occupancy Too High Restored</td>
<td>Facility Occupancy Too High Restored</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Failed to Report Expected Event</td>
<td>Failed to Report Expected Event</td>
</tr>
<tr>
<td>Fire Alarm</td>
<td>Fire Alarm</td>
</tr>
<tr>
<td>Fire Alarm Acknowledge</td>
<td>Fire Alarm Acknowledge</td>
</tr>
<tr>
<td>Fire Alarm Acknowledged Clear</td>
<td>Fire Alarm Acknowledged Clear</td>
</tr>
<tr>
<td>Fire Alarm Block Acknowledge</td>
<td>Fire Alarm Block Acknowledge</td>
</tr>
<tr>
<td>Fire Alarm In</td>
<td>Fire Alarm In</td>
</tr>
<tr>
<td>Fire Alarm Out</td>
<td>Fire Alarm Out</td>
</tr>
<tr>
<td>Fire Button Set</td>
<td>Fire Button Set</td>
</tr>
<tr>
<td>Fire Missing</td>
<td>Fire Missing</td>
</tr>
<tr>
<td>Fire Walk Test Ended</td>
<td>Fire Walk Test Ended</td>
</tr>
<tr>
<td>Fire Walk Test Started</td>
<td>Fire Walk Test Started</td>
</tr>
<tr>
<td>Fire Zone Walk Tested</td>
<td>Fire Zone Walk Tested</td>
</tr>
<tr>
<td>Firmware Download Started</td>
<td>Firmware Download Started</td>
</tr>
<tr>
<td>Firmware Download Completed</td>
<td>Firmware Download Completed</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Firmware Download Failed</td>
<td>Firmware Download Failed</td>
</tr>
<tr>
<td>First Card Unlock Mode Denied: Blocked Mode</td>
<td>First Card Unlock Mode Denied: Blocked Mode</td>
</tr>
<tr>
<td>First Card Unlock Mode Denied: Secured Mode</td>
<td>First Card Unlock Mode Denied: Secured Mode</td>
</tr>
<tr>
<td>First Card Unlock Mode Disabled</td>
<td>First Card Unlock Mode Disabled</td>
</tr>
<tr>
<td>First Card Unlock Mode Enabled</td>
<td>First Card Unlock Mode Enabled</td>
</tr>
<tr>
<td>Foil Break Alarm</td>
<td>Foil Break Alarm</td>
</tr>
<tr>
<td>Foil Break Restore</td>
<td>Foil Break Restore</td>
</tr>
<tr>
<td>Foodstamps Tender</td>
<td>Foodstamps Tender</td>
</tr>
<tr>
<td>Gasoline Prepayment</td>
<td>Gasoline Prepayment</td>
</tr>
<tr>
<td>Gasoline Prepayment Refund</td>
<td>Gasoline Prepayment Refund</td>
</tr>
<tr>
<td>Generic Event</td>
<td>Generic Event</td>
</tr>
<tr>
<td>Global Linkage Action Executed</td>
<td>Global Linkage Action Executed</td>
</tr>
<tr>
<td>Global Linkage Action Failed</td>
<td>Global Linkage Action Failed</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Granted Access</td>
<td>Access Granted</td>
</tr>
<tr>
<td>Granted APB Violation, Entry Made</td>
<td>Access Granted Anti-Passback Used</td>
</tr>
<tr>
<td>Granted APB Violation, No Entry Made</td>
<td>Access Granted Anti-Passback Not Used</td>
</tr>
<tr>
<td>Granted Facility Code</td>
<td>Access Granted On Facility Code</td>
</tr>
<tr>
<td>Granted Facility Code, No Entry</td>
<td>Access Granted On Facility Code No Entry Made</td>
</tr>
<tr>
<td>Granted No Entry</td>
<td>Access Granted No Entry Made</td>
</tr>
<tr>
<td>Granted Under Duress</td>
<td>Access Granted Under Duress</td>
</tr>
<tr>
<td>Granted Under Duress, No Entry</td>
<td>Access Granted Under Duress - No Entry Made</td>
</tr>
<tr>
<td>Grounded Loop Active</td>
<td>Grounded Loop Alarm Active</td>
</tr>
<tr>
<td>Grounded Loop Restored</td>
<td>Cancelled Grounded Loop</td>
</tr>
<tr>
<td>Guard Tour Action Executed</td>
<td>Guard Tour Action Executed</td>
</tr>
<tr>
<td>Guard Tour Action Failed</td>
<td>Guard Tour Action Failed</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>History Report End</td>
<td>History Report End</td>
</tr>
<tr>
<td>History Report Start</td>
<td>History Report Start</td>
</tr>
<tr>
<td>Hold</td>
<td>Hold</td>
</tr>
<tr>
<td>Holdup Alarm Restore</td>
<td>Holdup Alarm Restore</td>
</tr>
<tr>
<td>Host Executed Function List</td>
<td>Host Executed Function List</td>
</tr>
<tr>
<td>Host Open Door - Door Used</td>
<td>Host Open Door - Door Used</td>
</tr>
<tr>
<td>Host Open Door - Door Not Used</td>
<td>Host Open Door - Door Not Used</td>
</tr>
<tr>
<td>In-Camera-Memory Download Completed</td>
<td>In-Camera-Memory Download Completed</td>
</tr>
<tr>
<td>In-Camera-Memory Download Failed</td>
<td>In-Camera-Memory Download Failed</td>
</tr>
<tr>
<td>In-Camera-Memory Download Restored</td>
<td>In-Camera-Memory Download Restored</td>
</tr>
<tr>
<td>In-Camera-Memory Download Started</td>
<td>In-Camera-Memory Download Started</td>
</tr>
<tr>
<td>Inactive Badge</td>
<td>Inactive Badge</td>
</tr>
<tr>
<td>Incoming Call</td>
<td>Incoming Call</td>
</tr>
<tr>
<td>Information Message</td>
<td>Information Message</td>
</tr>
<tr>
<td>Initiated</td>
<td>Initiated</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Input Bypassed</td>
<td>Input Bypassed</td>
</tr>
<tr>
<td>Input Disabled</td>
<td>Input Disabled</td>
</tr>
<tr>
<td>Input Masked</td>
<td>Input Masked</td>
</tr>
<tr>
<td>Input Restored</td>
<td>Input Restored</td>
</tr>
<tr>
<td>Input Unmasked</td>
<td>Input Unmasked</td>
</tr>
<tr>
<td>Intercom Function</td>
<td>Intercom Function</td>
</tr>
<tr>
<td>Interlock Area Busy</td>
<td>Interlock Area Busy</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Insufficient Frame Rate Detected</td>
<td>N/A</td>
</tr>
<tr>
<td>Insufficient Frame Rate Restored</td>
<td>N/A</td>
</tr>
<tr>
<td>Intrusion Command Accepted</td>
<td>Intrusion Command</td>
</tr>
<tr>
<td></td>
<td>Accepted</td>
</tr>
<tr>
<td>Intrusion Command Denied</td>
<td>Intrusion Command</td>
</tr>
<tr>
<td></td>
<td>Denied</td>
</tr>
<tr>
<td>Invalid Access Level</td>
<td>Invalid Access</td>
</tr>
<tr>
<td>Invalid Badge</td>
<td>Invalid Badge</td>
</tr>
<tr>
<td>Invalid Camera</td>
<td>Invalid Camera</td>
</tr>
<tr>
<td>Invalid Camera Restored</td>
<td>Invalid Camera</td>
</tr>
<tr>
<td>Invalid Card Format</td>
<td>Invalid Card Format</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Invalid Device Serial Number</td>
<td>Invalid Device Serial Number</td>
</tr>
<tr>
<td>Invalid Facility Code</td>
<td>Invalid Facility Code</td>
</tr>
<tr>
<td>Invalid Issue Code</td>
<td>Invalid Issue Code</td>
</tr>
<tr>
<td>Invalid OEM Code</td>
<td>Invalid OEM Code</td>
</tr>
<tr>
<td>Invalid PIN Number</td>
<td>Invalid PIN Number</td>
</tr>
<tr>
<td>Item Correct of Previously entered Item</td>
<td>Item Correct of Previously entered Item</td>
</tr>
<tr>
<td>Item Sold</td>
<td>Item Sold</td>
</tr>
<tr>
<td>IVS Channel Processing Failed</td>
<td>IVS Channel Processing Failed</td>
</tr>
<tr>
<td>IVS Channel Processing Restarted</td>
<td>IVS Channel Processing Restarted</td>
</tr>
<tr>
<td>IVS Connection Lost</td>
<td>IVS Connection Lost</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>IVS Connection Restored</td>
<td>IVS Connection Restored</td>
</tr>
<tr>
<td>IVS Engine Connection Lost</td>
<td>IVS Engine Connection Lost</td>
</tr>
<tr>
<td>IVS Engine Connection Restored</td>
<td>IVS Engine Connection Restored</td>
</tr>
<tr>
<td>Key Override</td>
<td>Key Override</td>
</tr>
<tr>
<td>Keypad Fire</td>
<td>Keypad Fire</td>
</tr>
<tr>
<td>Lamp Test Activated</td>
<td>Lamp Test Activated</td>
</tr>
<tr>
<td>Lamp Test Completed</td>
<td>Lamp Test Completed</td>
</tr>
</tbody>
</table>
### Alarm Event Table

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
<th>Duress*</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Will Soon Expire - X Days Left</td>
<td>License Will Soon Expire - X Days Left</td>
<td>System</td>
<td>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, refer to <strong>Send an E-mail</strong> on page 163.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>Line Error Active</td>
<td>Line Error Active</td>
<td>System</td>
<td>Generated when a line error fault condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Line Error Restored</td>
<td>Cancelled Line Error</td>
<td>System</td>
<td>Generated when the line error fault condition was restored.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Local I/O Executed Function List</td>
<td>Local I/O Executed Function List</td>
<td>System</td>
<td>Generated when a local I/O function list has been activated.</td>
<td></td>
</tr>
<tr>
<td>Loitering</td>
<td>Loitering</td>
<td>Video</td>
<td>Generated when a loiterer is detected.</td>
<td></td>
</tr>
<tr>
<td>Loitering Restored</td>
<td>Loitering Restored</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of a Loitering event.</td>
<td></td>
</tr>
<tr>
<td>Lock Initialized</td>
<td>Lock Initialized</td>
<td>System</td>
<td>Lock was initialized using the PP (Portable Programmer) application.</td>
<td></td>
</tr>
<tr>
<td>Lock Updated</td>
<td>Lock Updated</td>
<td>System</td>
<td>Lock was updated.</td>
<td></td>
</tr>
<tr>
<td>Lock Powered Up by Portable Programmer</td>
<td>Lock Powered Up by Portable Programmer</td>
<td>System</td>
<td>Generated after a power up by the portable programmer.</td>
<td></td>
</tr>
<tr>
<td>Locked Under AFC</td>
<td>Locked Under AFC</td>
<td>System</td>
<td>End of AFC state.</td>
<td></td>
</tr>
<tr>
<td>Locked Under First Card Unlock</td>
<td>Locked Under First Card Unlock</td>
<td>System</td>
<td>First card unlock mode; door is relocked.</td>
<td></td>
</tr>
<tr>
<td>Lottery Pay Out</td>
<td>Lottery Pay Out</td>
<td>POS</td>
<td>Generated when a lottery pay out has occurred.</td>
<td></td>
</tr>
<tr>
<td>Low Battery</td>
<td>Low Battery</td>
<td>System</td>
<td>Low battery alarm.</td>
<td></td>
</tr>
<tr>
<td>Low Battery Restored</td>
<td>Low Battery Restored</td>
<td>System</td>
<td>Generated when a low battery is restored.</td>
<td></td>
</tr>
<tr>
<td>Lottery Sale</td>
<td>Lottery Sale</td>
<td>POS</td>
<td>Generated when an event for a lottery sale has occurred.</td>
<td></td>
</tr>
<tr>
<td>Low Voltage</td>
<td>Low Voltage</td>
<td>System</td>
<td>Generated when a low voltage condition has been detected at the device.</td>
<td></td>
</tr>
<tr>
<td>Low Voltage Restored</td>
<td>Low Voltage Restored</td>
<td>System</td>
<td>Generated when a device resumes its proper voltage.</td>
<td></td>
</tr>
<tr>
<td>Manufacturer Coupon</td>
<td>Manufacturer Coupon</td>
<td>POS</td>
<td>Indicates a manufacturer coupons.</td>
<td></td>
</tr>
<tr>
<td>Manufacturer Coupon Redemption</td>
<td>Manufacturer Coupon Redemption</td>
<td>POS</td>
<td>Transaction generated for a manufacturer coupon redemption.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress^*</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Max Assets Reached</td>
<td>Max Assets Reached</td>
<td>System</td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>Max Biometric Templates Reached</td>
<td>Max Biometric Templates Reached</td>
<td>System</td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>Max Cardholders Reached</td>
<td>Max Cardholders Reached</td>
<td>System</td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>Merchandise Returned</td>
<td>Merchandise Returned</td>
<td>POS</td>
<td>Generated when merchandise is returned.</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous Tender</td>
<td>Miscellaneous Tender</td>
<td>POS</td>
<td>Generated when miscellaneous tender is used.</td>
<td></td>
</tr>
<tr>
<td>Module Active</td>
<td>Module Active</td>
<td>Fire</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Module Clear</td>
<td>Module Clear</td>
<td>Fire</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Motion Detected (AI)</td>
<td>Motion Detected (AI)</td>
<td>Video</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Motion Detected (AI) Restored</td>
<td>Motion Detected (AI) Restored</td>
<td>Video</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Muster Mode Reset</td>
<td>Muster Mode Reset</td>
<td>Mustering</td>
<td>Generated when muster mode is reset.</td>
<td></td>
</tr>
<tr>
<td>Muster Mode Start</td>
<td>Muster Mode Start</td>
<td>Mustering</td>
<td>Generated when muster mode is started.</td>
<td></td>
</tr>
<tr>
<td>Negative Tax</td>
<td>Negative Tax</td>
<td>POS</td>
<td>Generated when negative tax is used.</td>
<td></td>
</tr>
<tr>
<td>Negative Total</td>
<td>Negative Total</td>
<td>POS</td>
<td>Generated when there is a negative total.</td>
<td></td>
</tr>
<tr>
<td>Network Utilization Threshold Exceeded</td>
<td>Network Utilization Threshold Exceeded</td>
<td>System</td>
<td>Generated by an LNVR recorder when current Network activity levels exceeds the user defined limit.</td>
<td></td>
</tr>
<tr>
<td>Network Utilization Threshold Restored</td>
<td>Network Utilization Threshold Restored</td>
<td>System</td>
<td>Generated by an LNVR recorder when the current Network activity level dropped below the user defined limit.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>No Biometric Template Data</td>
<td>No Biometric Template Data</td>
<td>Biometric</td>
<td>Generated when no biometric template data was available from the biometric reader at the end of a verification sequence.</td>
<td></td>
</tr>
<tr>
<td>No Blocking Override</td>
<td>No Blocking Override</td>
<td></td>
<td>User does not have Blocked override privilege.</td>
<td></td>
</tr>
<tr>
<td>Non-Fire Active</td>
<td>Non-Fire Active</td>
<td>System</td>
<td>An event indicating a non fire related alarm condition is active.</td>
<td></td>
</tr>
<tr>
<td>Non-Fire Active Cleared</td>
<td>Non-Fire Active Cleared</td>
<td>System</td>
<td>An event indicating a non fire related alarm condition is no longer active.</td>
<td></td>
</tr>
<tr>
<td>Not Configured</td>
<td>Not Configured</td>
<td>System</td>
<td>Generated when a device has not been configured or defined by the host.</td>
<td></td>
</tr>
<tr>
<td>No Sale</td>
<td>No Sale</td>
<td>POS</td>
<td>Transaction generated for a no sale.</td>
<td></td>
</tr>
<tr>
<td>Object Crosses a Region</td>
<td>Object Crosses a Region</td>
<td>Video</td>
<td>Generated when an object is detected in the process of crossing a user-specified region.</td>
<td></td>
</tr>
<tr>
<td>Object Crosses a Region Restored</td>
<td>Object Crosses a Region Restored</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of an Object Crosses a Region event.</td>
<td></td>
</tr>
<tr>
<td>Object Detection</td>
<td>Object Detection</td>
<td>Video</td>
<td>Generated when an object complying with user-specifications is detected.</td>
<td></td>
</tr>
<tr>
<td>Object Detection Restored</td>
<td>Object Detection Restored</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of an Object Detection event.</td>
<td></td>
</tr>
<tr>
<td>Object Left Behind</td>
<td>Object Left Behind</td>
<td>Video</td>
<td>Generated when a foreground object is left for more than a pre-specified duration.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Object Left Behind</td>
<td>Object Left Behind</td>
<td>Video</td>
<td>Generated when the left object was taken or the background (after a certain time interval) is relearned.</td>
<td></td>
</tr>
<tr>
<td>Restored</td>
<td>Restored</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Lurking</td>
<td>Object Lurking</td>
<td>Video</td>
<td>Generated when a moving object stops or slows down for at least 7 seconds.</td>
<td></td>
</tr>
<tr>
<td>Object Lurking Restored</td>
<td>Object Lurking Restored</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of an Object Lurking event.</td>
<td></td>
</tr>
<tr>
<td>Object Moves Too Fast</td>
<td>Object Moves Too Fast</td>
<td>Video</td>
<td>Generated when a moving object is detected in a scene with a speed that exceeds the user-specified rate.</td>
<td></td>
</tr>
<tr>
<td>Object Moves Too Fast</td>
<td>Object Moves Too Fast</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of an Object Moves Too Fast event.</td>
<td></td>
</tr>
<tr>
<td>Object Moves Too Fast</td>
<td>Object Moves Too Fast</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of an Object Moves Too Fast event.</td>
<td></td>
</tr>
<tr>
<td>Object Moves Too Fast</td>
<td>Object Moves Too Fast</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of an Object Moves Too Fast event.</td>
<td></td>
</tr>
<tr>
<td>Object Starts to Move</td>
<td>Object Starts to Move</td>
<td>Video</td>
<td>Generated when a monitored object begins moving.</td>
<td></td>
</tr>
<tr>
<td>Object Starts to Move</td>
<td>Object Starts to Move</td>
<td>Video</td>
<td>Generated 8 seconds after last detection of an Object Starts to Move event.</td>
<td></td>
</tr>
<tr>
<td>Object Starts to Move</td>
<td>Object Starts to Move</td>
<td>Video</td>
<td>Generated 8 seconds after last detection of an Object Starts to Move event.</td>
<td></td>
</tr>
<tr>
<td>Object Starts to Move</td>
<td>Object Starts to Move</td>
<td>Video</td>
<td>Generated 8 seconds after last detection of an Object Starts to Move event.</td>
<td></td>
</tr>
<tr>
<td>Object Removed</td>
<td>Object Removed</td>
<td>Video</td>
<td>Generated when a background object is removed.</td>
<td></td>
</tr>
<tr>
<td>Object Removed Restored</td>
<td>Object Removed Restored</td>
<td>Video</td>
<td>Generated when the object is returned to its original location or the background (after a certain time interval) is relearned.</td>
<td></td>
</tr>
<tr>
<td>Object Stops</td>
<td>Object Stops</td>
<td>Video</td>
<td>Generated when a foreground object stops.</td>
<td></td>
</tr>
<tr>
<td>Object Stops Restored</td>
<td>Object Stops Restored</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of an Object Stops event.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Open Door Command Issued - Door Used</td>
<td>Open Door Command Issued - Door Used</td>
<td>System</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Open Door Command Issued - Door Not Used</td>
<td>Open Door Command Issued - Door Not Used</td>
<td>System</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Open Line Active</td>
<td>Open Line Active</td>
<td>System</td>
<td>Generated when an open line fault condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Open Line Restored</td>
<td>Cancelled Open Line</td>
<td>System</td>
<td>Generated when the open line fault condition was restored.</td>
<td></td>
</tr>
<tr>
<td>Override Preprogrammed Price</td>
<td>Override Preprogrammed Price</td>
<td>POS</td>
<td>Generated when the preprogrammed price is overridden.</td>
<td></td>
</tr>
<tr>
<td>Panel Download Completed</td>
<td>Full Panel Download Completed</td>
<td>System</td>
<td>Generated when a database download to the controller has completed.</td>
<td></td>
</tr>
<tr>
<td>Panel Download Started</td>
<td>Full Panel Download Started</td>
<td>System</td>
<td>Generated when a database download to the controller has started.</td>
<td></td>
</tr>
<tr>
<td>Panel Event Capacity Exceeded - Events Overwritten</td>
<td>Panel Event Capacity Exceeded - Events Overwritten</td>
<td>System</td>
<td>Generated when the event log in the panel fills up and starts overwriting old events.</td>
<td></td>
</tr>
<tr>
<td>Panel Free Memory Low</td>
<td>Panel Free Memory Low</td>
<td>System</td>
<td>Generated when the free memory in the panel (controller) is below what is determined to be a safe value.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Panel ID Mismatch</td>
<td>Panel ID Mismatch</td>
<td>System</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Panel Marked Offline After Timeout</td>
<td>Panel Marked Offline After Timeout</td>
<td>System</td>
<td>Generated when the video recorder is automatically placed offline because a connection cannot be made after the user specified amount of time.</td>
<td></td>
</tr>
<tr>
<td>Panel Options Mismatch</td>
<td>Panel Options Mismatch</td>
<td>System</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Panel Power Up Complete</td>
<td>Panel Power Up Complete</td>
<td>System</td>
<td>Generated when the panel power up is complete.</td>
<td></td>
</tr>
<tr>
<td>Panic Abort</td>
<td>Panic Abort</td>
<td>Trouble</td>
<td>Generated when a panic alarm has been manually aborted/canceled.</td>
<td></td>
</tr>
<tr>
<td>Panic Alarm</td>
<td>Panic Alarm</td>
<td>Trouble</td>
<td>Generated when emergency assistance has been manually requested.</td>
<td></td>
</tr>
<tr>
<td>Panic Alarm Restore</td>
<td>Panic Alarm Restore</td>
<td>Trouble</td>
<td>Generated when the panic alarm has been restored.</td>
<td></td>
</tr>
<tr>
<td>Pay Out</td>
<td>Pay Out</td>
<td>POS</td>
<td>Generated when a payout takes place.</td>
<td></td>
</tr>
<tr>
<td>Payment of Refund to Customer</td>
<td>Payment of Refund to Customer</td>
<td>POS</td>
<td>Generated when a payment or refund is given to a customer.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Payment Toward Charge Account Balance</td>
<td>Payment Toward Charge Account Balance</td>
<td>POS</td>
<td>Generated when a payment toward an account balance.</td>
<td></td>
</tr>
<tr>
<td>People Counting</td>
<td>People Counting</td>
<td>Video</td>
<td>Generated when the count was updated (usually within a short delay after an individual passes).</td>
<td></td>
</tr>
<tr>
<td>People Entry Rate Too High</td>
<td>People Entry Rate Too High</td>
<td>Video</td>
<td>Generated when the number of entering people rises above the limit during the specified time interval.</td>
<td></td>
</tr>
<tr>
<td>People Entry Rate Too High Restored</td>
<td>People Entry Rate Too High Restored</td>
<td>Video</td>
<td>Generated when the number of entering people returns to a value below the limit during the specified time interval.</td>
<td></td>
</tr>
<tr>
<td>People Entry Rate Too Low</td>
<td>People Entry Rate Too Low</td>
<td>Video</td>
<td>Generated when the number of entering people falls below the limit during the specified time interval.</td>
<td></td>
</tr>
<tr>
<td>People Entry Rate Too Low Restored</td>
<td>People Entry Rate Too Low Restored</td>
<td>Video</td>
<td>Generated when the number of entering people returns to a value above the limit during the specified time interval.</td>
<td></td>
</tr>
<tr>
<td>People Exit Rate Too High</td>
<td>People Exit Rate Too High</td>
<td>Video</td>
<td>Generated when the number of exiting people rises above the limit during the specified time interval.</td>
<td></td>
</tr>
<tr>
<td>People Exit Rate Too High Restored</td>
<td>People Exit Rate Too High Restored</td>
<td>Video</td>
<td>Generated when the number of exiting people returns to a value below the limit during the specified time interval.</td>
<td></td>
</tr>
<tr>
<td>People Exit Rate Too Low</td>
<td>People Exit Rate Too Low</td>
<td>Video</td>
<td>Generated when the number of exiting people falls below the limit during the specified time interval.</td>
<td></td>
</tr>
<tr>
<td>People Exit Rate Too Low Restored</td>
<td>People Exit Rate Too Low Restored</td>
<td>Video</td>
<td>Generated when the number of exiting people returns to a value above the limit during the specified time interval.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Pick Up</td>
<td>Pick Up</td>
<td>POS</td>
<td>Transaction indicating a pick up has occurred.</td>
<td></td>
</tr>
<tr>
<td>Point Enabled</td>
<td>Point Enabled</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Point Disabled</td>
<td>Point Disabled</td>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poor Video Visibility</td>
<td>N/A</td>
<td>N/A</td>
<td>Generated when the video quality returns to an acceptable level.</td>
<td></td>
</tr>
<tr>
<td>Poor Video Visibility</td>
<td>Cancelled Power Failure</td>
<td>System</td>
<td>Generated when the power failure condition was restored.</td>
<td></td>
</tr>
<tr>
<td>Power Failure Active</td>
<td>Power Failure</td>
<td>System</td>
<td>Generated when a power failure condition has been detected.</td>
<td></td>
</tr>
<tr>
<td>Power Failure Restored</td>
<td>Cancelled Power Failure</td>
<td>System</td>
<td>Generated when the power failure condition was restored.</td>
<td></td>
</tr>
<tr>
<td>Pre-Alarm</td>
<td>Pre-Alarm</td>
<td>System</td>
<td>An event indicating a pre-alarm condition is active.</td>
<td></td>
</tr>
<tr>
<td>Pre-Alarm Clear</td>
<td>Pre-Alarm Clear</td>
<td>System</td>
<td>An event indicating a pre-alarm condition is no longer active.</td>
<td></td>
</tr>
<tr>
<td>Price Lookup</td>
<td>Price Lookup</td>
<td>POS</td>
<td>Generated when a price lookup has taken place.</td>
<td></td>
</tr>
<tr>
<td>Quantity or Weight</td>
<td>Quantity or Weight</td>
<td>POS</td>
<td>An event indicating a quantity or weight.</td>
<td></td>
</tr>
<tr>
<td>Reader Input Tamper</td>
<td>Reader Input Tamper</td>
<td>System</td>
<td>Generated when the reader input tamper has gone active.</td>
<td></td>
</tr>
<tr>
<td>Reader Low Battery</td>
<td>Reader Low Battery</td>
<td>System</td>
<td>Reader low battery alarm.</td>
<td></td>
</tr>
<tr>
<td>Reader Low Battery</td>
<td>Reader Low Battery Restored</td>
<td>System</td>
<td>Generated when a reader low battery is restored.</td>
<td></td>
</tr>
<tr>
<td>Reader Input Tamper</td>
<td>Reader Input Tamper Cancelled</td>
<td>System</td>
<td>Generated when the reader input tamper was restored.</td>
<td></td>
</tr>
<tr>
<td>Reader Mode Blocked</td>
<td>Reader Mode Blocked</td>
<td>System</td>
<td>Lock has entered blocked mode.</td>
<td></td>
</tr>
<tr>
<td>Reader Mode Secured</td>
<td>Reader Mode Secured</td>
<td>System</td>
<td>Lock has entered secured mode.</td>
<td></td>
</tr>
<tr>
<td>Reader Mode Unsecured</td>
<td>Reader Mode Unsecured</td>
<td>System</td>
<td>Lock has entered unsecured mode.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Reader Mode Card and Pin</td>
<td>Reader Mode Card and Pin</td>
<td>System</td>
<td>Generated when the reader mode has changed to “Pin and Card” for the device.</td>
<td></td>
</tr>
<tr>
<td>Reader Mode Card Only</td>
<td>Reader Mode Card Only</td>
<td>System</td>
<td>Generated when the reader mode has changed to “Card Only.”</td>
<td></td>
</tr>
<tr>
<td>Reader Mode Facility Code</td>
<td>Reader Mode Facility Code</td>
<td>System</td>
<td>Generated when the reader mode has changed to “Facility Code Only.”</td>
<td></td>
</tr>
<tr>
<td>Reader Mode First Card Unlock</td>
<td>Reader Mode First Card Unlock</td>
<td>System</td>
<td>Generated when the reader mode has changed to “First Card Unlock.”</td>
<td></td>
</tr>
<tr>
<td>Reader Mode Locked</td>
<td>Reader Mode Locked</td>
<td>System</td>
<td>Generated when the reader mode has changed to “Locked.”</td>
<td></td>
</tr>
<tr>
<td>Reader Mode Pin or Card</td>
<td>Reader Mode Pin or Card</td>
<td>System</td>
<td>Generated when the reader mode has changed to “Pin or Card” for the device.</td>
<td></td>
</tr>
<tr>
<td>Reader Mode Unlocked</td>
<td>Reader Mode Unlocked</td>
<td>System</td>
<td>Generated when the reader mode has changed to “Unlocked.”</td>
<td></td>
</tr>
<tr>
<td>Reader Module Firmware Upgraded</td>
<td>Reader Module Firmware Upgraded</td>
<td>System</td>
<td>Reader firmware has been updated.</td>
<td></td>
</tr>
<tr>
<td>Reader Motor Stalled</td>
<td>Reader Motor Stalled</td>
<td>System</td>
<td>Generated when the motor stalls on a reader.</td>
<td></td>
</tr>
<tr>
<td>Reader Motor Stalled Restored</td>
<td>Reader Motor Stalled Restored</td>
<td>System</td>
<td>Generated when a motor stalled condition has been restored.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Reader Reset</td>
<td>Reader Reset</td>
<td>System</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Realtime Clock Updated</td>
<td>Realtime Clock</td>
<td>System</td>
<td>The Real Time Clock (RTC) was updated.</td>
<td></td>
</tr>
<tr>
<td>Register X Report</td>
<td>Register X Report</td>
<td>POS</td>
<td>Indicates a X report was generated. X reports are financial, end of day, clerk, etc. reports.</td>
<td></td>
</tr>
<tr>
<td>Register Z Report</td>
<td>Register Z Report</td>
<td>POS</td>
<td>Indicates a Z report was generated. Z reports are the same as X reports, but resets totals to zero.</td>
<td></td>
</tr>
<tr>
<td>Rejected Biometric Score</td>
<td>Rejected Biometric Score</td>
<td>Biometric</td>
<td>This event returns the rejected biometric score (the actual denied event is sent separately).</td>
<td></td>
</tr>
<tr>
<td>Relay Contact Activated</td>
<td>Relay Contact</td>
<td>System</td>
<td>Generated when a relay contact was activated.</td>
<td></td>
</tr>
<tr>
<td>Relay Contact Deactivated</td>
<td>Relay Contact</td>
<td>System</td>
<td>Generated when a relay contact was deactivated.</td>
<td></td>
</tr>
<tr>
<td>Removed Object</td>
<td>Removed Object</td>
<td>Video</td>
<td>Generated when an object which was part of the background is detected as missing.</td>
<td></td>
</tr>
<tr>
<td>Removed Object Restored</td>
<td>Removed Object</td>
<td>Video</td>
<td>Generated when the object is returned to its original location or the background (after a certain time interval) is relearned.</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
<td>Duress*</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Request to Exit - Door Used</td>
<td>Request to Exit - Door Used</td>
<td>System</td>
<td>Generated when the request to exit is granted and the door is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> If the <strong>Assumed Door Used</strong> checkbox is selected on the Readers form, then the door is assumed to be used. This might interfere with this event.</td>
<td></td>
</tr>
<tr>
<td>Request to Exit - Door Not Used</td>
<td>Request to Exit - Door Not Used</td>
<td>System</td>
<td>Generated when the request to exit is granted and the door is not used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> If the <strong>Assumed Door Used</strong> checkbox is selected on the Readers form, then the door is assumed to be used. This might interfere with this event.</td>
<td></td>
</tr>
<tr>
<td>Retrieved</td>
<td>Retrieved</td>
<td>Intercom</td>
<td>Generated when a phone call is retrieved/answered.</td>
<td></td>
</tr>
<tr>
<td>Ringing</td>
<td>Ringing</td>
<td>Intercom</td>
<td>Generated when an intercom station/phone is ringing.</td>
<td></td>
</tr>
<tr>
<td>Runaway Device</td>
<td>Runaway Device</td>
<td>System</td>
<td>Generated when the conditions specified for a runaway state are met. These conditions are configured on the System Options &gt; Runaway Detection tab in System Administration.</td>
<td></td>
</tr>
<tr>
<td>Runaway Device Restored</td>
<td>Runaway Device Restored</td>
<td>System</td>
<td>Generated when the conditions configured for runaway detection are no longer true.</td>
<td></td>
</tr>
</tbody>
</table>
## Alarm Monitoring User Guide

### 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.

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running Out of Disk Space</td>
<td>Running Out of Disk Space</td>
<td>NetDVMS</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Subtotal</td>
<td>Sales Subtotal</td>
<td>POS</td>
<td>A transaction that reports the sale subtotal.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Change</td>
<td>Schedule Change</td>
<td>System</td>
<td>Generated when a schedule, added in the Scheduler, is changed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Executed</td>
<td>Schedule Executed</td>
<td>System</td>
<td>Generated when a schedule, added in the Scheduler, is executed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler Action Executed</td>
<td>Scheduler Action Executed</td>
<td>System</td>
<td>Generated when a scheduler action has executed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler Action Failed</td>
<td>Scheduler Action Failed</td>
<td>System</td>
<td>Generated when a scheduler action has failed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Alarm Acknowledge</td>
<td>Security Alarm Acknowledge</td>
<td>Fire</td>
<td>Generated when a security alarm has been acknowledged.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Alarm Block Acknowledge</td>
<td>Security Alarm Block Acknowledge</td>
<td>Fire</td>
<td>Generated when all security alarms have been acknowledged at the fire panel.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Alarm In</td>
<td>Security Alarm In</td>
<td>Fire</td>
<td>Generated when a new security alarm has been detected for the device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Alarm Out</td>
<td>Security Alarm Out</td>
<td>Fire</td>
<td>Generated when a device with a previous security alarm has returned to its normal state.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shorted Line Active</td>
<td>Shorted Line Active</td>
<td>System</td>
<td>Generated when a shorted line fault condition has been detected.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Shorted Line Restored</td>
<td>Canceled Shorted Line</td>
<td>System</td>
<td>Generated when a device with a shorted line fault condition has returned to its normal state.</td>
</tr>
<tr>
<td>Signal Silence</td>
<td>Signal Silence</td>
<td>Fire</td>
<td>Generated when the alarm signal on the hardware has been silenced.</td>
</tr>
<tr>
<td>Smart Card Authentication Failed</td>
<td>Smart Card Authentication Failed</td>
<td>System</td>
<td>Generated when a smart card authentication failed.</td>
</tr>
<tr>
<td>Smart VMD</td>
<td>Smart VMD</td>
<td>Video</td>
<td>Generated when a change is detected.</td>
</tr>
<tr>
<td>Smart VMD Restored</td>
<td>Smart VMD Restored</td>
<td>Video</td>
<td>Generated 8 seconds after the last detection of a Smart VMD event.</td>
</tr>
<tr>
<td>Status In</td>
<td>Status In</td>
<td>Fire</td>
<td>Generated when a status reporting device is active.</td>
</tr>
<tr>
<td>Status - Missing Fire Supervision</td>
<td>Status - Missing Fire Supervision</td>
<td>Fire</td>
<td>Fire supervision is missing.</td>
</tr>
<tr>
<td>Status Out</td>
<td>Status Out</td>
<td>Fire</td>
<td>Generated when a status reporting device has returned to the inactive state.</td>
</tr>
<tr>
<td>Storage Failure</td>
<td>Storage Failure</td>
<td>Video</td>
<td>Indicates that something is wrong related to recording/retrieving video to/from hard drives. Includes LNVR database failure.</td>
</tr>
<tr>
<td>Store Coupon</td>
<td>Store Coupon</td>
<td>POS</td>
<td>Indicates a store coupon.</td>
</tr>
<tr>
<td>Supervisory Acknowledge</td>
<td>Supervisory Acknowledge</td>
<td>Fire</td>
<td>Generated when a supervisory condition has been acknowledged.</td>
</tr>
<tr>
<td>Supervisory Block Acknowledge</td>
<td>Supervisory Block Acknowledge</td>
<td>Fire</td>
<td>Generated when all supervisory conditions have been acknowledged at the fire panel.</td>
</tr>
<tr>
<td>Supervisory In</td>
<td>Supervisory In</td>
<td>Fire</td>
<td>Generated when a new supervisory condition has been detected for the device.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Supervisory Out</td>
<td>Supervisory Out</td>
<td>Fire</td>
<td>Generated when a device with a previous supervisory condition has returned to its normal state.</td>
</tr>
<tr>
<td>System Reset</td>
<td>System Reset</td>
<td>Fire</td>
<td>Generated when the fire panel has been reset.</td>
</tr>
<tr>
<td>Tax Amount</td>
<td>Tax Amount</td>
<td>POS</td>
<td>Event that indicates the tax amount.</td>
</tr>
<tr>
<td>Taxable Subtotal</td>
<td>Taxable Subtotal</td>
<td>POS</td>
<td>Transaction that reports the taxable subtotal</td>
</tr>
<tr>
<td>Timeout Exceeded - No Second Card</td>
<td>Timeout Exceeded - No Second Card</td>
<td>Area Control</td>
<td>Generated when no second card was presented within the time limit for the area/reader using two-man control.</td>
</tr>
<tr>
<td>Time Out-Of-Sync</td>
<td>Time Out-Of-Sync</td>
<td>Video</td>
<td>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.</td>
</tr>
<tr>
<td>Time Out-Of-Sync Restored</td>
<td>Time Out-Of-Sync Restored</td>
<td>Video</td>
<td>Generated when the time difference between the camera and video recorder returns to less than 20 seconds.</td>
</tr>
<tr>
<td>Total Amount Due</td>
<td>Total Amount Due</td>
<td>POS</td>
<td>Transaction indicating the total amount due.</td>
</tr>
<tr>
<td>Transaction Number</td>
<td>Transaction Number</td>
<td>POS</td>
<td>Event Generated that indicates the transaction number of the sales transaction.</td>
</tr>
<tr>
<td>Transfer, Diagnostics</td>
<td>Transfer, Diagnostics</td>
<td>System</td>
<td>Generated when a user is connected to the device for diagnostic purposes.</td>
</tr>
<tr>
<td>Transfer, History</td>
<td>Transfer, History</td>
<td>System</td>
<td>Generated when a history data was transferred from the device to the parent device.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Transfer, PDA To Lock</td>
<td>Transfer, PDA To Lock</td>
<td>System</td>
<td>Generated when the device (lockset) is programmed/reprogrammed through a download from a Mobile Configurator.</td>
</tr>
<tr>
<td>Transferred Call</td>
<td>Intercom</td>
<td></td>
<td>Generated if an intercom call is transferred.</td>
</tr>
<tr>
<td>Transmitter Alarm</td>
<td>Transmitter Alarm</td>
<td>Transmitter</td>
<td>Generated when the button or input on a transmitter has been activated.</td>
</tr>
<tr>
<td>Transmitter Alarm RESTORED</td>
<td>Transmitter Alarm RESTORED</td>
<td>Transmitter</td>
<td>Generated when the transmitter alarm has been restored.</td>
</tr>
<tr>
<td>Transmitter Inactivity</td>
<td>Transmitter Inactivity</td>
<td>Transmitter</td>
<td>Transmitter has been inactive longer than the supervision interval</td>
</tr>
<tr>
<td>Transmitter Low Battery</td>
<td>Transmitter Low Battery</td>
<td>Transmitter</td>
<td>Transmitter low battery alarm</td>
</tr>
<tr>
<td>Transmitter Low Battery RESTORED</td>
<td>Transmitter Low Battery RESTORED</td>
<td>Transmitter</td>
<td>Generated when a transmitter low battery has been restored.</td>
</tr>
<tr>
<td>Transmitter Pre-Tilt</td>
<td>Transmitter Pre-Tilt</td>
<td>Transmitter</td>
<td>Generated when the transmitter is in the pre-tilt state.</td>
</tr>
<tr>
<td>Transmitter Pre-Tilt RESTORED</td>
<td>Transmitter Pre-Tilt RESTORED</td>
<td>Transmitter</td>
<td>Generated when the transmitter has returned to normal from the pre-tilt state.</td>
</tr>
<tr>
<td>Transmitter Pull Cord Alarm</td>
<td>Transmitter Pull Cord Alarm</td>
<td>Transmitter</td>
<td>Generated when the pull cord on a transmitter has been pulled and is in alarm.</td>
</tr>
<tr>
<td>Transmitter Pull Cord RESTORED</td>
<td>Transmitter Pull Cord RESTORED</td>
<td>Transmitter</td>
<td>Generated when the transmitter pull cord alarm has been restored.</td>
</tr>
<tr>
<td>Transmitter Tamper</td>
<td>Transmitter Tamper</td>
<td>Transmitter</td>
<td>Transmitter tamper alarm.</td>
</tr>
<tr>
<td>Transmitter Tamper RESTORED</td>
<td>Transmitter Tamper RESTORED</td>
<td>Transmitter</td>
<td>Generated when a transmitter tamper has been restored.</td>
</tr>
<tr>
<td>Transmitter Temporary Tilt Disable</td>
<td>Transmitter Temporary Tilt Disable</td>
<td>Transmitter</td>
<td>Generated when the transmitter temporary tilt has been disabled.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Transmitter Tilt</td>
<td>Transmitter Tilt</td>
<td>Transmitte</td>
<td></td>
</tr>
<tr>
<td><strong>(Disabled)</strong></td>
<td><strong>Disabled</strong></td>
<td>r</td>
<td>Generated when the transmitter tilt function has been disabled.</td>
</tr>
<tr>
<td>Transmitter Tilt</td>
<td>Transmitter Tilt</td>
<td>Transmitte</td>
<td></td>
</tr>
<tr>
<td><strong>(Enabled)</strong></td>
<td><strong>Enabled</strong></td>
<td>r</td>
<td>Generated when the transmitter tilt function has been enabled.</td>
</tr>
<tr>
<td>Transmitter Tilt</td>
<td>Transmitter Tilt</td>
<td>Transmitte</td>
<td></td>
</tr>
<tr>
<td><strong>(Restored)</strong></td>
<td><strong>Restored</strong></td>
<td>r</td>
<td>Generated when the tilt condition on the transmitter has been restored.</td>
</tr>
<tr>
<td>Transmitter Acknowle</td>
<td>Transmitter Acknowledge</td>
<td>Transmitte</td>
<td>This event is reported when an alarm generated by a transmitter has been</td>
</tr>
<tr>
<td>dge</td>
<td></td>
<td>r</td>
<td>acknowledged.</td>
</tr>
<tr>
<td>Transmitter No</td>
<td>Transmitter No</td>
<td>Transmitte</td>
<td>This event is reported when an alarm generated by a transmitter has not</td>
</tr>
<tr>
<td>Response</td>
<td>Response</td>
<td>r</td>
<td>been acknowledged.</td>
</tr>
<tr>
<td>Transmitter Touch</td>
<td>Transmitter Touch</td>
<td>Transmitte</td>
<td>Alarm generated by a transmitter when the item it is protecting is</td>
</tr>
<tr>
<td>Alarm</td>
<td>Alarm</td>
<td>r</td>
<td>touched.</td>
</tr>
<tr>
<td>Transmitter Removal</td>
<td>Transmitter Removal</td>
<td>Transmitte</td>
<td>Alarm generated by a transmitter when an item it is protecting is removed.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Alarm</td>
<td>r</td>
<td></td>
</tr>
<tr>
<td>Trouble Acknowledge</td>
<td>Trouble Acknowledge</td>
<td>Fire</td>
<td>Generated when the trouble condition has been acknowledged.</td>
</tr>
<tr>
<td>Trouble Acknowledge Clear</td>
<td>Trouble Acknowledge Clear</td>
<td>Fire</td>
<td>Generated when a trouble condition that has been cleared from the system has</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>been acknowledged by a user.</td>
</tr>
<tr>
<td>Trouble Bell #</td>
<td>Trouble Bell 1 or 2</td>
<td>Relay/Soun</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore</td>
<td>der</td>
<td>Generated when Trouble bell 1 or 2 is restored.</td>
</tr>
<tr>
<td>Trouble Bell #</td>
<td>Trouble Bell 1 or 2</td>
<td>Relay/Soun</td>
<td></td>
</tr>
<tr>
<td>Restore</td>
<td>Restore</td>
<td>der</td>
<td>Generated when Trouble bell 1 or 2 is in alarm.</td>
</tr>
<tr>
<td>Trouble Block</td>
<td>Trouble Block</td>
<td>Fire</td>
<td>Generated when all trouble conditions have been acknowledged at the fire</td>
</tr>
<tr>
<td>Acknowledge</td>
<td>Acknowledge</td>
<td></td>
<td>panel.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trouble In</td>
<td>Trouble In</td>
<td>Fire</td>
<td>Generated when a new trouble condition has been detected for the device.</td>
</tr>
<tr>
<td>Trouble Out</td>
<td>Trouble Out</td>
<td>Fire</td>
<td>Generated when a device with a previous trouble condition has returned to its normal state.</td>
</tr>
<tr>
<td>Unanswered Call</td>
<td>Unanswered Call</td>
<td>Intercom</td>
<td>Generated if a ringing intercom call goes unanswered.</td>
</tr>
<tr>
<td>Unexpected Access</td>
<td>Unexpected Access</td>
<td>System</td>
<td>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.</td>
</tr>
<tr>
<td>Unexpected Access Attempt</td>
<td>Unexpected Access Attempt</td>
<td>System</td>
<td>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.</td>
</tr>
<tr>
<td>Unknown Elevator Terminal</td>
<td>Unknown Elevator Terminal</td>
<td>System</td>
<td>Generated when an elevator terminal is detected that has not been configured in the system.</td>
</tr>
<tr>
<td>Unknown User Command</td>
<td>Unknown User Command</td>
<td>System</td>
<td>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.</td>
</tr>
<tr>
<td>Unlocked Under AFC</td>
<td>Unlocked Under AFC</td>
<td>System</td>
<td>Lock has entered AFC state.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unlocked Mode Change Denied: Blocked Mode</td>
<td>Unlocked Mode Change Denied: Blocked Mode</td>
<td>System</td>
<td>Automatic scheduled change to unlocked mode was denied because lock is in blocked mode.</td>
</tr>
<tr>
<td>Unlocked Mode Change Denied: Low Battery</td>
<td>Unlocked Mode Change Denied: Low Battery</td>
<td>System</td>
<td>Automatic scheduled change to unlocked mode was denied due to low battery condition.</td>
</tr>
<tr>
<td>Unlocked Mode Change Denied: Secured Mode</td>
<td>Unlocked Mode Change Denied: Secured Mode</td>
<td>System</td>
<td>Automatic scheduled change to unlocked mode was denied because lock is in secured mode.</td>
</tr>
<tr>
<td>Unlocked Under First Card Unlock</td>
<td>Unlocked Under First Card Unlock</td>
<td>System</td>
<td>First card unlock mode; door is unlocked.</td>
</tr>
<tr>
<td>Unsupported Hardware</td>
<td>Unsupported Hardware</td>
<td>System</td>
<td>Generated when hardware that is not supported is added to the system.</td>
</tr>
<tr>
<td>Untyped Abort</td>
<td>Untyped Abort</td>
<td>Trouble</td>
<td>Generated when an alarm for a device of an unknown type has been aborted/canceled.</td>
</tr>
<tr>
<td>Untyped Alarm</td>
<td>Untyped Alarm</td>
<td>Trouble</td>
<td>Generated when an alarm for a device of unknown type occurs.</td>
</tr>
<tr>
<td>Untyped Alarm Restore</td>
<td>Untyped Alarm Restore</td>
<td>Trouble</td>
<td>Generated when the device of an unknown type is restored.</td>
</tr>
<tr>
<td>Untyped Bypass</td>
<td>Untyped Bypass</td>
<td>Trouble</td>
<td>Generated when a device of an unknown type has been bypassed.</td>
</tr>
<tr>
<td>Update: Now able to Achieve Current Required Storage Setting</td>
<td>Update: Now able to Achieve Current Required Storage Setting</td>
<td>System</td>
<td>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.</td>
</tr>
<tr>
<td>Use Limit Exceeded</td>
<td>Use Limit Exceeded</td>
<td>Denied</td>
<td>Access was denied because the use limit for the badge has been exceeded.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Failed to Reach Destination</td>
<td>User Failed to Reach Destination</td>
<td>System</td>
<td>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.</td>
</tr>
<tr>
<td>User Generated Video Event</td>
<td>User Generated Video Event</td>
<td>Video</td>
<td>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.</td>
</tr>
<tr>
<td>Value Added</td>
<td>Value Added</td>
<td>POS</td>
<td>Event that indicates value added.</td>
</tr>
<tr>
<td>Video Event Threshold Reached</td>
<td>Video Event Threshold Reached</td>
<td>Video</td>
<td>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.)</td>
</tr>
<tr>
<td>Video Failover Failed</td>
<td>Video Failover Failed</td>
<td>Video</td>
<td>Generated when the camera is configured for failover and failover cannot be activated on this camera.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Video Failover Restored</td>
<td>Video Failover Restored</td>
<td>Video</td>
<td>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.</td>
</tr>
<tr>
<td>Video Failover Started</td>
<td>Video Failover Started</td>
<td>Video</td>
<td>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.</td>
</tr>
<tr>
<td>Video Grinstead Restored</td>
<td>N/A</td>
<td>N/A</td>
<td>Displayed after noise (graininess) in the video has been reduced.</td>
</tr>
<tr>
<td>Video Overflow Restored</td>
<td>Video Overflow Restored</td>
<td>Video</td>
<td>Generated when the recorder is no longer having troubles handling incoming video.</td>
</tr>
<tr>
<td>Video Overflow Started</td>
<td>Video Overflow Started</td>
<td>Video</td>
<td>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.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Video Server Disk Full</td>
<td>Video Server Disk Full</td>
<td>Video</td>
<td>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.</td>
</tr>
<tr>
<td>Video Server is Not Recording</td>
<td>Video Server is Not Recording</td>
<td>Video</td>
<td>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.</td>
</tr>
<tr>
<td>Video Source Signal Lost</td>
<td>Video Source Signal Lost</td>
<td>Video</td>
<td>Generated when the video signal from a channel is lost from the video server. This alarm may be accompanied by a Communications Lost alarm.</td>
</tr>
<tr>
<td>Video Source Signal Restored</td>
<td>Video Source Signal Restored</td>
<td>Video</td>
<td>Generated when the video signal from a channel is restored to the video server. This alarm may be accompanied by a Communications Restored alarm.</td>
</tr>
<tr>
<td>Video Storage Unavailable</td>
<td>Video Storage Unavailable</td>
<td>Video</td>
<td>Generated when the recorder cannot record video to a drive.</td>
</tr>
<tr>
<td>Void or Error Correction</td>
<td>Void or Error Correction</td>
<td>POS</td>
<td>Transaction that indicates a void or error correction</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>----------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Walk Test ##</td>
<td>Walk Test ##</td>
<td>Fire</td>
<td>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.</td>
</tr>
<tr>
<td>Walk Test Uninstalled</td>
<td>Walk Test Uninstalled</td>
<td>Fire</td>
<td>Generated when the reported device was part of a walk test and has been physically disconnected from the system.</td>
</tr>
<tr>
<td>Walk Test Unprogrammed</td>
<td>Walk Test Unprogrammed</td>
<td>Fire</td>
<td>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).</td>
</tr>
<tr>
<td>Walk Test Untest</td>
<td>Walk Test Untest</td>
<td>Fire</td>
<td>Generated when the reported device is no longer being tested (part of a walk test).</td>
</tr>
<tr>
<td>Warning: Unable to Meet Required Storage Setting</td>
<td>Warning: Unable to Meet Required Storage Setting</td>
<td>System</td>
<td>Generated by an LNVR recorder when video storage will be full in less number of days than defined by the user.</td>
</tr>
<tr>
<td>Warning: Unable to Meet Required Storage Setting! Deleting Oldest Video</td>
<td>Warning: Unable to Meet Required Storage Setting! Deleting Oldest Video</td>
<td>System</td>
<td>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.</td>
</tr>
<tr>
<td>Warning: Poor Visibility</td>
<td>N/A</td>
<td>N/A</td>
<td>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.</td>
</tr>
</tbody>
</table>
The duress column marks which alarm events can be used as duress events if your system is configured for duress.

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning: Video Graininess</td>
<td>N/A</td>
<td>N/A</td>
<td>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.</td>
</tr>
<tr>
<td>Wireless Smoke Detector</td>
<td>Wireless Smoke Detector</td>
<td>Fire</td>
<td>A wireless smoke detector has generated an alarm.</td>
</tr>
<tr>
<td>WLM Firmware Upgraded</td>
<td>WLM Firmware Upgraded</td>
<td>System</td>
<td>Radio module firmware was updated</td>
</tr>
</tbody>
</table>

* The duress column marks which alarm events can be used as duress events if your system is configured for duress.
## NGP Alarm/Event Descriptions

<table>
<thead>
<tr>
<th>Alarm Event</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Lockouts Removed</td>
<td>System</td>
<td>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.</td>
</tr>
<tr>
<td>Area Alarm - Confirmed</td>
<td>Area Control</td>
<td>Applies to panels configured in the UK (APCO). An unconfirmed alarm is when one input becomes active in a armed area.</td>
</tr>
<tr>
<td>Area Arm Failure</td>
<td>System</td>
<td>When the arming of an area fails.</td>
</tr>
<tr>
<td>Area Arm with Override</td>
<td>System</td>
<td>Generated when a user with Master Override permission in the assigned permission profile arms an area.</td>
</tr>
<tr>
<td>Area Confirm Alarm Reset</td>
<td>System</td>
<td>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.</td>
</tr>
<tr>
<td>Area Limit Minimum</td>
<td>Area Control</td>
<td></td>
</tr>
<tr>
<td>Armed Off</td>
<td>System</td>
<td>Arming has been turned OFF for the indicated Area (Disarmed).</td>
</tr>
<tr>
<td>Armed On</td>
<td>System</td>
<td>Arming has been turned ON for the indicated Area (Full Armed).</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Armed On with Bypasses</td>
<td>Armed On with Bypasses</td>
<td>System</td>
</tr>
<tr>
<td>Armed on with Isolates</td>
<td>Armed on with Isolates</td>
<td>System</td>
</tr>
<tr>
<td>Backup Battery Critical</td>
<td>Backup Battery Critical</td>
<td>System</td>
</tr>
<tr>
<td>Backup Battery Low</td>
<td>Backup Battery Low</td>
<td>System</td>
</tr>
<tr>
<td>Bad Card Lockout</td>
<td>Bad Card Lockout</td>
<td>System</td>
</tr>
<tr>
<td>Bad PIN Lockout</td>
<td>Bad PIN Lockout</td>
<td>System</td>
</tr>
<tr>
<td>Bad System ID</td>
<td>Bad System ID</td>
<td>System</td>
</tr>
<tr>
<td>Battery Restored</td>
<td>Battery Restored</td>
<td>System</td>
</tr>
<tr>
<td>Battery Trouble</td>
<td>Battery Trouble</td>
<td>System</td>
</tr>
<tr>
<td>Cannot Arm - Users Left In Area</td>
<td>Cannot Arm - Users Left In Area</td>
<td>System</td>
</tr>
<tr>
<td>Central Station Report Delay</td>
<td>Central Station Report Delay</td>
<td>System</td>
</tr>
<tr>
<td>Central Station Report Success</td>
<td>Central Station Report Success</td>
<td>System</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Command Point Failure</td>
<td>Command Point Failure</td>
<td>System</td>
</tr>
<tr>
<td>Command Point Reset</td>
<td>Command Point Reset</td>
<td>System</td>
</tr>
<tr>
<td>Command Point Trip</td>
<td>Command Point Trip</td>
<td>System</td>
</tr>
<tr>
<td>Config No Reply</td>
<td>Config No Reply</td>
<td>System</td>
</tr>
<tr>
<td>Denied - Area Out of Schedule</td>
<td>Denied - Area Out of Schedule</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Denied - Dual Custody Violation</td>
<td>Denied - Dual Custody Violation</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Denied - Group Mismatch</td>
<td>Denied - Group Mismatch</td>
<td>Access</td>
</tr>
<tr>
<td>Denied - No Off Authority</td>
<td>Denied - No Off Authority</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Denied - No On Authority</td>
<td>Denied - No On Authority</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Denied - No Stay Authority</td>
<td>Denied - No Stay Authority</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Denied - Pending Enroll</td>
<td>Denied - Pending Enroll</td>
<td>Access</td>
</tr>
<tr>
<td>Denied, duplicate card</td>
<td>Denied, duplicate card</td>
<td>System</td>
</tr>
<tr>
<td>Denied, duplicate card</td>
<td>Denied, duplicate card</td>
<td>Access</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Door Held Open Pre Alarm</td>
<td>Door Held Open Pre Alarm</td>
<td>System</td>
</tr>
<tr>
<td>Door Locked Out</td>
<td>Door Locked Out</td>
<td>System</td>
</tr>
<tr>
<td>Door Mag Trouble Clear</td>
<td>Door Mag Trouble Clear</td>
<td>System</td>
</tr>
<tr>
<td>Door Mag Trouble</td>
<td>Door Mag Trouble</td>
<td>System</td>
</tr>
<tr>
<td>Door Reinstated</td>
<td>Door Reinstated</td>
<td>System</td>
</tr>
<tr>
<td>Door Restore</td>
<td>Door Restore</td>
<td>System</td>
</tr>
<tr>
<td>Dual Custody User Off (Disarm)</td>
<td>Dual Custody User Off (Disarm)</td>
<td>System</td>
</tr>
<tr>
<td>Emergency Off</td>
<td>Emergency Off</td>
<td>System</td>
</tr>
<tr>
<td>Entry Exit</td>
<td>Entry Exit</td>
<td>System</td>
</tr>
<tr>
<td>Fap Processing Start</td>
<td>Fap Processing Start</td>
<td>System</td>
</tr>
<tr>
<td>Grant Last User (Override)</td>
<td>Grant Last User (Override)</td>
<td>Access</td>
</tr>
<tr>
<td>Granted-Dual Custody</td>
<td>Granted-Dual Custody</td>
<td>Access</td>
</tr>
<tr>
<td>Granted-Escort</td>
<td>Granted-Escort</td>
<td>Access</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Granted-Exit-Dual Custody</td>
<td>Granted-Exit-Dual Custody</td>
<td>Access Granted</td>
</tr>
<tr>
<td>Granted-Exit-Escort</td>
<td>Granted-Exit-Escort</td>
<td>Access Granted</td>
</tr>
<tr>
<td>Granted-Exit-Master</td>
<td>Granted-Exit-Master</td>
<td>Access Granted</td>
</tr>
<tr>
<td>Granted-Master</td>
<td>Granted-Master</td>
<td>Access Granted</td>
</tr>
<tr>
<td>Granted-Pending Entry</td>
<td>Granted-Pending Entry</td>
<td>Access Granted</td>
</tr>
<tr>
<td>HSC Reset</td>
<td>HSC Reset</td>
<td>System</td>
</tr>
<tr>
<td>HSC-IP Trouble</td>
<td>HSC-IP Trouble</td>
<td>System</td>
</tr>
<tr>
<td>HSC-IP Restored</td>
<td>HSC-IP Restored</td>
<td>System</td>
</tr>
<tr>
<td>Isolate</td>
<td>Isolate</td>
<td>System</td>
</tr>
<tr>
<td>Memory Backup</td>
<td>Memory Backup</td>
<td>System</td>
</tr>
<tr>
<td>Battery Low</td>
<td>Battery Low</td>
<td>System</td>
</tr>
<tr>
<td>No Escort Authority</td>
<td>No Escort Authority</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>No Intrusion Off or Stay Authority</td>
<td>No Intrusion Off or Stay Authority</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Output Error</td>
<td>Output Error</td>
<td>System</td>
</tr>
<tr>
<td>Panel Reboot to Factory Defaults</td>
<td>Panel Reboot to Factory Defaults</td>
<td>System</td>
</tr>
<tr>
<td>Panel Reset Watchdog</td>
<td>Panel Reset Watchdog</td>
<td>System</td>
</tr>
<tr>
<td>Panel Restart Due to Power Failure</td>
<td>Panel Restart Due to Power Failure</td>
<td>System</td>
</tr>
<tr>
<td>Pending first user</td>
<td>Pending first user</td>
<td>System</td>
</tr>
<tr>
<td>POD Trouble</td>
<td>POD Trouble</td>
<td>System</td>
</tr>
<tr>
<td>Point Test Fail</td>
<td>Point Test Fail</td>
<td>System</td>
</tr>
<tr>
<td>Reader Authority Toggle</td>
<td>Reader Authority Toggle</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Reader in Dual Custody Mode</td>
<td>Reader in Dual Custody Mode</td>
<td>System</td>
</tr>
<tr>
<td>Reader in Escort Mode</td>
<td>Reader in Escort Mode</td>
<td>System</td>
</tr>
<tr>
<td>Reader Mode PIN Only</td>
<td>Reader Mode PIN Only</td>
<td>System</td>
</tr>
<tr>
<td>Reader in Normal Mode</td>
<td>Reader in Normal Mode</td>
<td>System</td>
</tr>
<tr>
<td>Reader Toggle</td>
<td>Reader Toggle</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Schedule Resumed</td>
<td>Schedule Resumed</td>
<td>System</td>
</tr>
<tr>
<td>Schedule Suspend</td>
<td>Schedule Suspend</td>
<td>System</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>SIA Session Code</td>
<td>SIA Session Code</td>
<td>System</td>
</tr>
<tr>
<td>Supply Fuse Restored</td>
<td>Supply Fuse Restored</td>
<td>System</td>
</tr>
<tr>
<td>Supply Fuse Trouble</td>
<td>Supply Fuse Trouble</td>
<td>System</td>
</tr>
<tr>
<td>System APB reset</td>
<td>System APB reset</td>
<td>System</td>
</tr>
<tr>
<td>System Confirm</td>
<td>System Confirm</td>
<td>System</td>
</tr>
<tr>
<td>System Confirm Alarm Reset</td>
<td>System Confirm Alarm Reset</td>
<td>System</td>
</tr>
<tr>
<td>System Message</td>
<td>System Message</td>
<td>System</td>
</tr>
<tr>
<td>System Password Fail</td>
<td>System Password Fail</td>
<td>System</td>
</tr>
<tr>
<td>System Program Changed</td>
<td>System Program Changed</td>
<td>System</td>
</tr>
<tr>
<td>System Program Fail</td>
<td>System Program Fail</td>
<td>System</td>
</tr>
<tr>
<td>System Restored</td>
<td>System Restored</td>
<td>System</td>
</tr>
<tr>
<td>System Trouble</td>
<td>System Trouble</td>
<td>System</td>
</tr>
<tr>
<td>System Unconfirm</td>
<td>System Unconfirm</td>
<td>System</td>
</tr>
<tr>
<td>Telco SIA/CID) Reset</td>
<td>Telco SIA/CID) Reset</td>
<td>System</td>
</tr>
<tr>
<td>Unauthorized Off</td>
<td>Unauthorized Off</td>
<td>System</td>
</tr>
<tr>
<td>Upload Okay</td>
<td>Upload Okay</td>
<td>System</td>
</tr>
<tr>
<td>Alarm</td>
<td>Event</td>
<td>Event Type</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>USB 1 Fuse Blown</td>
<td>USB 1 Fuse Blown</td>
<td>System</td>
</tr>
<tr>
<td>USB 1 Fuse Reset</td>
<td>USB 1 Fuse Reset</td>
<td>System</td>
</tr>
<tr>
<td>USB 2 Fuse Blown</td>
<td>USB 2 Fuse Blown</td>
<td>System</td>
</tr>
<tr>
<td>USB 2 Fuse Reset</td>
<td>USB 2 Fuse Reset</td>
<td>System</td>
</tr>
<tr>
<td>User APB Reset</td>
<td>User APB Reset</td>
<td>System</td>
</tr>
<tr>
<td>Verify User</td>
<td>Verify User</td>
<td>System</td>
</tr>
<tr>
<td>Wandering Patient Alarm Reset</td>
<td>Wandering Patient Alarm Reset</td>
<td>System</td>
</tr>
<tr>
<td>Wandering Patient at Door</td>
<td>Wandering Patient at Door</td>
<td>System</td>
</tr>
<tr>
<td>Warning - Users Left In Area</td>
<td>Warning - Users Left In Area</td>
<td>System</td>
</tr>
</tbody>
</table>
APPENDIX C  

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.

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 Guest Access to Readers
Listing of each Reader, and which cardholders have access to that reader. Includes the associated Access Level and Timezone.

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.
Description of Reports

**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.
Description of Reports

**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.
Description of Reports

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 D: LNVR Network Setup

The LNVR Network Setup tool allows you to enable multicast, fix computers with several network interfaces, and restrict ports usage as well as make them firewall friendly. Install the LNVR Network Setup tool by running LnrNI.exe from the directory: C:\Program Files\Common Files\Lenel. Alternatively, the tool is also provided on the Supplemental Materials disc under Current Digital Video.

Deliver Live Video to Alarm Monitoring Using IP Multicast Protocol

Using an IP Multicast protocol to send video is ideal because it saves bandwidth when more than one machine is watching the same video. IP Multicast video is sent once instead of multiple times as with a Unicast protocol.

Live video retrieval from LNVR recorders by default is configured to use UDP/IP, Multicast, and TCP/IP protocols on any available port. Clients can specify which of these protocol they want to use for each request. The options are to use:

- UDP/IP
- Multicast

If all protocols are selected to be used then your computer will try and use IP Multicast first but if it fails it will then use UDP/IP. If UDP/IP fails then TCP/IP will be used.

---

Note: While you can select to not use UDP/IP and Multicast, TCP/IP is always used as a last resort if the previous methods fail.

---

Note: Recorded video is always retrieved using DCOM protocol. DCOM is also used to access LNVR recorder for configuration. It is assumed that DCOM is configured properly and therefore this document does not cover retrieval of recorded video.

---

To configure your system to use IP Multicast you must:

- Configure Recorder for IP Multicast
- Configure Client for IP Multicast
- Configure Router for IP Multicast
- Configure Firewall for IP Multicast
**LNVR Network Setup Window**

The LNVR Network Setup tool has three tabs that are viewable if you have the specific network setups. If you only see one or two of the following tabs do not worry. They are not applicable for your system.

**Client Network Settings Form**

The Client Network Settings form can be used by all machines and allows you to specify how the client computer receives video data. You can also enable and disable multicast and UDP/IP use.

---

**Note:** The Client Network Settings form only affects client applications. It will not change anything on the server.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Network Interface</td>
<td>Lists the network interface you wish to setup for LNVR Live Video if your computer has more than one network card.</td>
</tr>
<tr>
<td>Connection Protocol Settings</td>
<td>Area where you select what protocol settings you want to use. These include using Multicast and UDP/IP. You can also choose what ports to use with UDP/IP.</td>
</tr>
<tr>
<td>Use Multicast</td>
<td>Select for client machines if you wish to use Multicast. Multicast allows more than one computer to view the same video. While this frees up bandwidth some routers and firewalls don’t allow this sort of multicast packets to pass through them.</td>
</tr>
<tr>
<td>Use UDP/IP</td>
<td>Select for client machines if you wish to use UDP/IP. UDP/IP allows more than one computer to view the same video. Unlike multicast, though, the video will be sent multiple times which will increase the network load.</td>
</tr>
<tr>
<td>Limit port range</td>
<td>Choose which ports should be used for UDP/IP.</td>
</tr>
</tbody>
</table>
Recorder Network Settings Form

The Recorder Network Settings form can only be used by LNVR machines and allows you to specify the ports used when client computers connect to them using TCP/IP.

**Important:** Multiple recorders should not use the same multicast ports. Doing so causes video frames from the recorders to conflict with each other and become interlaced. Each channel on a recorder should be given its own port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorder TCP/IP Port</td>
<td>The port used for the LNVR recorder.</td>
</tr>
<tr>
<td>Any Available</td>
<td>Select if you want the LNVR recorder to use any available port on the system.</td>
</tr>
<tr>
<td>Specific</td>
<td>Select if you want the LNVR recorder to use a specific port if firewalls prevent you from using any port.</td>
</tr>
<tr>
<td>First Recorder Multicast Port</td>
<td>The port used for the LNVR first recorder.</td>
</tr>
<tr>
<td>Any Available</td>
<td>Select if you want the LNVR first recorder to use any available port on the system.</td>
</tr>
<tr>
<td>Specific</td>
<td>Select if you want the LNVR first recorder to use a specific port if firewalls prevent you from using any port.</td>
</tr>
</tbody>
</table>
IVS Network Settings Form

The IVS Network Settings form can only be used by IVS machines and allows you to specify the ports used when client computers connect to them using TCP/IP.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntelligentVideo Server TCP/IP Port</td>
<td>The port used for the IVS servers.</td>
</tr>
<tr>
<td>Any Available</td>
<td>Select to use any available port when using TCP/IP with IVS machines.</td>
</tr>
<tr>
<td>Specific</td>
<td>Select to use a specific port when using TCP/IP with IVS machines if firewalls prevent you from using any port.</td>
</tr>
</tbody>
</table>

LNVR Network Setup Configurations

Configure Recorder for IP Multicast

1. Navigate to the directory: `C:\Program Files\Common Files\Lenel`.
2. Double-click on `LnrNI.exe` to run the LNVR Network Setup tool.
3. Alternatively, run the LNVR Network Setup tool from the Supplemental Materials disc.
4. If it has more than one network interface select the one you would like to use to send multcasts.
5. Click [Apply].
Configure Client for IP Multicast

1. Run the LNVR Network Setup tool from `C:\Program Files\Common Files\Lenel\LnrNI.exe` or from the Supplemental Materials disc on each OnGuard computer that is going to use Alarm Monitoring to see live video.

2. Select the **Use Multicast** check box.

3. Click [Apply].

Configure Router for IP Multicast

Most network routers and network devices between LNVR and its clients block IP Multicast traffic. Refer to the device manual of your specific equipment to see how to enable Multicast on it.

Configure Firewall for IP Multicast

A Firewall between LNVR and its clients can and usually does block both UDP/IP and IP Multicast traffic. This traffic is one directional communication, so if there are firewalls between LNVR and its clients they must have UDP/IP and IP Multicast traffic enabled from LNVR to its clients.

It is enough to open ports in one direction only (from LNVR to clients). If a firewall cannot be configured to enable UDP/IP traffic on all ports then a range of ports can be opened instead.

---

**Note:** A client will be able to see no more live video streams from the recorder than number of open ports.
Appendix E: Exporting Video

The OnGuard installation includes a conversion utility that converts exported video from the LDVR or LNVR native format to an “.asf” format. The “.asf” file format is playable on any machine that has Microsoft’s Windows Media Player and does not require any additional software to play video. The video converter is located at: C:\Program files\Common Files\LenelLVConvert.exe.

You can run the conversion utility either from a command line or by launching the utility. To use the standalone video conversion utility to export video, refer to Convert and Export Video on page 510.

The video converter is also available from within the VideoViewer and Alarm Monitoring applications. When used standalone, the source file can be changed in the Lenel Video Converter window; when used in Alarm Monitoring and VideoViewer it cannot. To use the video converter in VideoViewer or Alarm Monitoring to export video, refer to Export Video to a File on page 509.
**Lenel Video Converter Window**

<table>
<thead>
<tr>
<th>Form Element</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source file</td>
<td>Identifies the export file to be converted to the Windows Media format.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The <strong>Source file</strong> and <strong>Output file</strong> fields cannot be modified in Alarm Monitoring or VideoViewer; they can only be modified when using the standalone version of the video converter.</td>
</tr>
<tr>
<td>Browse</td>
<td>Search for the export file to be converted to the Windows Media format.</td>
</tr>
<tr>
<td>Output file</td>
<td>Name of the new file to be created.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The <strong>Source file</strong> and <strong>Output file</strong> fields cannot be modified in Alarm Monitoring or VideoViewer; they can only be modified when using the standalone version of the video converter.</td>
</tr>
<tr>
<td>Browse</td>
<td>Search for the location the new file should be created in.</td>
</tr>
<tr>
<td>Generate Overlay Image</td>
<td>If enabled, additional information such as time and date will be overlaid on the video image. If this check box is selected, the default is to show the date and time in the top-left corner.</td>
</tr>
<tr>
<td>Customize</td>
<td>Enables the user to customize the format and the content of overlay information.</td>
</tr>
<tr>
<td>Status area</td>
<td>Updates as the video is exported to show how much video has been exported and how much video still needs to be exported.</td>
</tr>
<tr>
<td>Convert</td>
<td>Converts the file from its native format to an “.asf” format.</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the window without converting the file from its native format to an “.asf” format.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays online help.</td>
</tr>
</tbody>
</table>
# Video Export Dialog

![Video Export Dialog Image]

<table>
<thead>
<tr>
<th>Form Element</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Type</td>
<td>Specifies the format for the exported video:</td>
</tr>
<tr>
<td></td>
<td>• Native Format - video format determined by the video recorder</td>
</tr>
<tr>
<td></td>
<td>• Windows Media Format - overlay may be applied to the video</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>Specifies whether the watermarking uses the default or custom key/signature. For more information, refer to <a href="#">Authenticate a Video File with Watermarking</a> on page 511.</td>
</tr>
<tr>
<td>Custom Signature</td>
<td>Specifies a custom digital key/signature.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Custom Signature is case sensitive.</td>
</tr>
<tr>
<td>File Name</td>
<td>Search for the location the new file should be created in.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text entered in this field will be displayed during the digital signature verification process.</td>
</tr>
<tr>
<td>Generate Overlay Image</td>
<td>If enabled, additional information such as time and date will be overlaid on the video image. If this check box is selected, the default is to show the date and time in the top-left corner.</td>
</tr>
<tr>
<td>Customize</td>
<td>Enables the user to customize the format and the content of overlay information.</td>
</tr>
<tr>
<td>Export</td>
<td>Saves the recorded video to a file using the configured options.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Aborts the export after the process has begun.</td>
</tr>
<tr>
<td>Close</td>
<td>Exits the dialog without exporting the video.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays online help.</td>
</tr>
</tbody>
</table>
**Customize Overlay Information Dialog**

![Customize Overlay Information Dialog Image]

<table>
<thead>
<tr>
<th>Form Element</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Location</td>
<td>Identifies which corner(s) the date will be printed. Possible values are top-left, top-right, bottom-left, bottom-right, and none. If none is selected, the field will not be shown. The default is to show the date and time in the top-left corner and no text.</td>
</tr>
<tr>
<td>Time Location</td>
<td>Identifies which corner(s) the time will be printed. Possible values are top-left, top-right, bottom-left, bottom-right, and none. If none is selected, the field will not be shown. The default is to show the date and time in the top-left corner and no text.</td>
</tr>
<tr>
<td>Text Location</td>
<td>Identifies which corner(s) the additional text will be printed. Possible values are top-left, top-right, bottom-left, bottom-right, and none. If none is selected, the field will not be shown. The default is to show the date and time in the top-left corner and no text.</td>
</tr>
<tr>
<td>Row fields</td>
<td>If more than one piece of information is printed in the same corner, this field allows you to specify if one item should appear above the other one. If the items are on the same row, they will be printed one after the other.</td>
</tr>
<tr>
<td>Text</td>
<td>Enter any additional text that you want to appear in the video. For example, the text could identify the location where the video came from.</td>
</tr>
<tr>
<td>Change</td>
<td>Allows the user to specify a different font, style, and color of the printed information.</td>
</tr>
<tr>
<td>Transparency</td>
<td>Specifies the transparency level of the printed text where 0 means the text is invisible and 100 means the text is opaque.</td>
</tr>
<tr>
<td>OK</td>
<td>Accepts the changes and closes the dialog.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Closes the dialog without applying any changes.</td>
</tr>
<tr>
<td>Load Settings</td>
<td>Loads a previously saved overlay configuration.</td>
</tr>
<tr>
<td>Save Settings</td>
<td>Saves an overlay configuration.</td>
</tr>
</tbody>
</table>
Video Conversion Procedures

The following procedures are used to convert, export and play video clips.

Note: The conversion utility converts “.lnr” or “.info/.spfs” files into “.asf” format.

Export Video to a File

This procedure describes using the video converter in VideoViewer or Alarm Monitoring. When using the standalone video conversion utility, refer to Convert and Export Video on page 510.

Recorded video and audio can be saved/exported to a file. By default the video clip is saved as “.asf” which can be played on any Microsoft Windows Media Player. In addition, video clips can be saved in Lenel proprietary formats. For LDVR hardware, proprietary formats include “.info” and “.spfs” files and for LNVR hardware the proprietary format is “.lnr” files.

Note: If you have video files in proprietary formats, you can use the conversion utility available at: C:\Program Files\Common Files\Lenel\LVConvert.exe.

1. While viewing recorded video in the Video Player, select Set Start/End Date from the Options menu.
2. The Date/Time window opens. Fill in the appropriate dates and times and click [OK].
3. From the Options menu select Export Video. The Video Export Dialog is displayed.
4. Select the Output Type from the drop-down list. The specific file type is determined in step 5.
5. Click the [...] button to browse for a location to save the exported video file. The Save As window opens.
   a. Select the file location.
   b. Enter the file name.
   c. Select the desired file format (*.asf), (*.info), (*.spfs), or (*.lnr).
Note: The file formats available in the drop down list reflect the output type chosen in Step 4.

d. Click [Save].

6. The Windows Media Format allows the use of an overlay image.
   a. Select the **Generate Overlay Image** check box to overlay the time and date on the video image.
   b. To customize the content of overlay information, click [Customize]. The Customize Information Overlay Dialog opens. For more information, refer to Customize Overlay Information Dialog on page 508.

7. Click [Export].

**Convert and Export Video**

This procedure describes using the standalone video conversion utility. When using the video converter in VideoViewer or Alarm Monitoring, refer to Export Video to a File on page 509.

The conversion utility is installed with OnGuard and can be executed from a command line as well as by launching the utility.

**Using the Conversion Utility**

1. Navigate to `C:\Program Files\Common Files\Lenel`.
2. Run the `LVConvert.exe` program in this directory.
3. The Video Converter window opens. Enter the source file name.
4. Enter the output file name.
5. **Optional** - Select and customize any overlay information.
6. Click [Convert].
7. Click [Close] when the conversion is complete.

Using a Command Line

1. Click Start, then select Run. The Run dialog opens.
2. Enter “LVConvert.exe -i InputFile.lnr -o OutputFile.asf [-c ConfigFile.xml] [-s]” where:
   - i specifies the input file
   - o specifies the output file
   - c (optional) specifies the overlay configuration file. If not specified, overlay information will not be generated.
   - s (optional) silent run. If specified the application will not pop up any error/status dialog boxes. This is useful if you are running the application as part of a script.
3. Click [OK].

Play Exported Video Clip Using Windows Media Player

1. Launch the Windows Media Player. On most Windows machines, you can do this by clicking Start, then Programs > Accessories > Entertainment > Windows Media Player.
2. On the File menu, select Open.
3. Type in the location of the video clip, or click on [Browse] to navigate to it.
4. Click [OK] (or [Open] if you browsed to the file). The video clip will be played in the Media Player window.

Authenticate a Video File with Watermarking

Embedding a watermark in the video file is equivalent to signing a digital identification on the content of the video. If the video is manipulated, the watermark is destroyed. The authenticator can verify whether a received video has been tampered with by attempting to match the signature.

The Watermarking feature allows the individual exporting the video to set a custom digital signature which can later be verified by the recipient of the video file.

Set a Watermark

1. From the Video Export Dialog in Alarm Monitoring or VideoViewer, select “Native Format” from the Output Type drop-down.
2. Select the type of signature, “Custom” or “Default”, from the Digital Signature drop-down list.
3. If you selected “Custom”, in the Custom Signature text box, enter a key for authentication (case sensitive). The recipient of the file will need to know this key to determine the validity of the video file.
Note: The Default signature type does not require a key for authentication.

4. Select other options as desired and click [Export] to finish. For more information, refer to Export Video to a File on page 509.

Authenticate the Watermark

Authentication of the watermark occurs with the stand-alone Lenel Video Player (LVPlayer.exe).

1. Navigate to the C:\Program Files\Common Files\Lenel directory and run LVPlayer.exe.
2. From the File menu, select Open File.
3. From the Control menu, select Verify Signature. The Signature Details dialog is displayed.
4. If a custom signature was entered during export, type the key entered in the Enter Signature text box.

Notes: The custom signature is case sensitive.

If the Default signature type was used during export the Enter Signature text box will be grayed out.

5. Click [Verify Signature]. A message will be displayed indicating whether the authentication was successful.
Appendix F: IntelligentAudio

IntelligentAudio performs audio analysis on forensic (live or recorded) video in Alarm Monitoring or VideoViewer. The Video Search can be used to monitor live or scan recorded video for audio events. Searches can be performed based on the type and volume of sound detected.

The Audio Level event can be configured in System Administration to trigger alarms in Alarm Monitoring. For more information, refer to the Digital Video Software User Guide.

Once Video Search is launched, select an IntelligentAudio event from the Event > Select Event > IntelligentAudio menu.

Audio Level

The Audio Level event identifies sound events crossing a volume threshold.

Event Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>Volume threshold for detection. Use the level displayed on the Event Feedback pane to determine a value appropriate to the scene.</td>
</tr>
<tr>
<td>Minimal Duration (seconds)</td>
<td>Length of time that sound should continue before an event is detected. The range of values is 0.010 to 10.000 seconds.</td>
</tr>
</tbody>
</table>

High Pitch Sounds

Typical high pitch sounds include: screams, sirens, squealing tires, etc.

Event Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td></td>
</tr>
<tr>
<td>Minimal Duration (seconds)</td>
<td>0.500</td>
</tr>
</tbody>
</table>
Impact Sounds

Typical impact sounds include: fallen object, crash, gunshot, etc.

**Event Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>Volume threshold for detection. Use the level displayed on the Event Feedback pane to determine a value appropriate to the scene.</td>
</tr>
<tr>
<td>Minimal Duration (seconds)</td>
<td>Length of time that sound should continue before an event is detected. The range of values is 0.060 to 10.000 seconds.</td>
</tr>
</tbody>
</table>

Unclassified Sounds

The Unclassified Sounds event can be used to detect sounds not classified as impact or high pitch. For example, undefined noise, speech, car starting, etc.

**Event Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>Volume threshold for detection. Use the level displayed on the Event Feedback pane to determine a value appropriate to the scene.</td>
</tr>
<tr>
<td>Minimal Duration (seconds)</td>
<td>Length of time that sound should continue before an event is detected. The range of values is 0.060 to 10.000 seconds.</td>
</tr>
</tbody>
</table>
This section contains information about using ILS locking solutions in Alarm Monitoring, in particular, the ILS wireless locking solution. For instructions on configuring the ILS locking solutions in OnGuard, refer to the System Administration User Guide.

### Offline Locks

Offline locks include the following types:

**ILS Offline Locks**. The lock operator reads the audits (events) from the ILS offline lock using the portable programmer (Mobile Configurator).

**ILS Integra Locks**. These are also offline locks. The lock operator reads the audits (events) from the ILS Integra lock using the portable programmer (XPP).

For more information on using ILS offline and ILS Integra locks in Alarm Monitoring, refer to the following:

- Retrieve Events from an ILS Offline Lock on page 516
- View ILS Offline Lock Events on page 516
- Show the Operator Column on page 516
- Retrieve Events from an ILS Integra Lock on page 516

### Wireless Locks

ILS wireless lock events are transmitted directly to Alarm Monitoring via the Wireless Gateway. You can also request wireless lock events on demand. For more information, refer to Retrieve Events from Wireless Locks on page 517.

For more information on using ILS wireless locks in Alarm Monitoring, refer to:

- Download ILS Wireless Locks on page 517
- Monitor ILS Wireless Lock Events on page 517
- View Wireless Lock Status on page 518
• Change Reader Access Modes on page 519
• Secure/Unsecure All Locks from a Reader Device Group on page 520
• View Wireless Diagnostics Information on page 521

For information on downloading ILS wireless firmware, refer to:
• Download Wireless Gateway Firmware on page 522
• Download ILS Wireless Lock Firmware on page 522

ILS Offline and ILS Integra Locks

Use the following procedures for ILS Offline and ILS Integra locks.

Retrieve Events from an ILS Offline Lock

Complete the following steps to see the offline lock events in Alarm Monitoring:

1. Read the audits (events) at the ILS offline lock using the Mobile Configurator.
2. Disconnect the Mobile Configurator from the lock, and then connect it to a workstation where Communication Server and Alarm Monitoring are running. The lock events will automatically display in the Main Alarm Monitor window.

IMPORTANT: If you are using a Mobile Configurator with OnGuard on a Windows XP or Windows 2003 system, Communication Server must be run as an application.

View ILS Offline Lock Events

When ILS offline lock events are uploaded from the Mobile Configurator to OnGuard:

• All other Mobile Configurators (ILS Offline panels) will show an online status in Alarm Monitoring.
• Events that have a lock operator associated with them will display with the operator name in the Operator column. By default, the Operator column is not shown.

Show the Operator Column

In order to enable this feature, complete the following steps:

1. Log into Alarm Monitoring.
2. Select Columns from the Configure menu.
3. Move “Operator” to the viewable columns list, and then click [OK].

Retrieve Events from an ILS Integra Lock

1. Read the audits (events) at the ILS Integra lock using the XPP portable programmer.
2. Disconnect the XPP from the lock, and then connect it to the workstation where it was configured. The lock events will automatically display in the Main Alarm Monitor window.
ILS Wireless Locks

Use the following procedures for ILS Wireless locks.

Retrieve Events from Wireless Locks

From Alarm Monitoring, complete the following steps:

1. Open the system status tree. From the View menu, select System Status, and then select a new or existing window. Expand the ILS wireless panel icon to show the locks assigned to it.

2. In the system status tree, complete either of the following steps:
   a. Right-click on an ILS wireless panel and then select Read Audits to upload the events of all locks assigned to that panel.
   b. (Optional) Right-click on an individual ILS wireless lock and then select Read Audits to upload the events of that lock, exclusively.

   When the Read Audits command is successfully issued, the Wireless Gateway adds the request to the queue to send at the next lock heartbeat at which time the latest lock events will display in Alarm Monitoring.

Download ILS Wireless Locks

ILS wireless locks can be downloaded from the Alarm Monitoring system status tree.

From Alarm Monitoring, complete the following steps:

1. Open the system status tree. From the View menu, select System Status, and then select an existing window or open a new one. Expand the segment node.

2. Right-click on the ILS wireless panel icon, and then select Download Database to directly download the data from the locks assigned to the Wireless Gateway.

3. (Optional) You can download the ILS wireless panels from the System Administration system tree, the Readers and Doors folder, or the Access Panels folder. For more information, refer to the System Administration User Guide.

Monitor ILS Wireless Lock Events

ILS wireless lock events are reported in Alarm Monitoring by way of four (4) 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 in the System Administration User Guide.
- 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 System Administration User Guide.
- From Alarm Monitoring, you can request to have non-priority events sent at the next heartbeat by issuing the Read Audits command. For more information, refer to Retrieve Events from Wireless Locks on page 517.
- The Mobile Configurator read events (audits) at the lock and uploads them to OnGuard.
View Wireless Lock Status

The Alarm Monitoring system status tree provides information about the ILS wireless lock including firmware version, battery level, (reader) access mode, deadbolt, door forced, and door held status, and the maximum number of cardholders that can be stored in the lock.

Status Updates When the Lock is Online

<table>
<thead>
<tr>
<th>Status</th>
<th>Updated Hardware Status</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware version</td>
<td>Yes</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Battery level</td>
<td>Yes</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Access mode</td>
<td>Yes</td>
<td>Reader mode changes such as Reader Mode Blocked, Reader Mode Card Only, Reader Mode Facility Code Only, Reader Mode First Card Unlock, and Reader Mode Unlocked.</td>
</tr>
<tr>
<td>Deadbolt</td>
<td>Yes</td>
<td>Internal Deadbolt On</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal Deadbolt Off</td>
</tr>
<tr>
<td>Door forced</td>
<td>Not applicable</td>
<td>Door Forced Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Door Forced Open Restored</td>
</tr>
<tr>
<td>Door held</td>
<td>Not applicable</td>
<td>Door Held Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Door Held Open Restored</td>
</tr>
</tbody>
</table>

Some of the lock status information depends on proper event handling. It is recommended that you configure lock events the affect lock status as priority one to ensure you are viewing live information. Otherwise, the corresponding events will not be updated until they are received. For more information, refer to Monitor ILS Wireless Lock Events on page 517.

Recommendations:

- Configure the deadbolt, door forced, and door held events as priority one, and make sure to include both members of the event set such as Door Held Open and Door Held Open Restored. For more information, refer to “Configure ILS Priority One Events” in the System Administration User Guide.
- Configure the reader mode change events as priority one.

Note: The maximum number of cardholders supported by the lock is calculated from the current cardholder (badge) data. For more information, refer to “Calculate Maximum Cardholders” in the System Administration User Guide.

Note: Battery level shows the percent of battery power remaining. This information is intended to provide an estimate but, if the battery level drops off significantly over a short period of time, it is recommended that you replace the batteries. For instructions on replacing the batteries, refer to the ILS Lock Operation User Guide.

From Alarm Monitoring, complete the following steps:

1. Open the system status tree. From the View menu, select System Status, and then select a new or existing window.
2. Expand the ILS wireless panel icon, and then view the status of each wireless lock assigned to that device.

**Change Reader Access Modes**

You can issue a command to change the reader access mode of ILS wireless locks. For more information, refer to Lock Operation Mode Changes in the ILS Lock Operation User Guide.

Choices include:

- **Card Only**: Sets the lock to card only mode.
- **Unlocked**: Sets the lock to unlocked mode.
- **Facility Code Only**: Sets the lock to facility code only mode.
- **First Card Unlock**: Sets the lock to first card unlock mode. The first card unlock mode is a qualifier for online Reader Mode. When updated, the online Reader Mode is in effect until the first (qualified) access granted with entry occurs. When the first access granted with entry occurs, the online Reader Mode changes to unlocked.
- **Blocked**: Sets the reader (lock) to blocked mode. When a lock is placed into blocked mode it remains locked for all cardholders except those with blocking override privileges. A lock can only be placed into blocked mode when the lock is in card only or unlocked mode. After exiting the blocked mode the lock returns to the mode it was in previous to entering the blocked mode unless there is an automatic scheduled change.
- **Secure**: Sets the lock to secure mode and locks the door.
- **Unsecure**: Sets the lock to unsecure mode and unlocks the door following a secured lock.

**Note:** The lock can also be put into or taken out of Blocked, Secure, or Unsecure mode by presenting a Blocking, Emergency Lock, or Emergency Unlock card. For more information, refer to Special Purpose Cards in the System Administration User Guide.

From Alarm Monitoring, complete the following steps:

1. Open the system status tree. From the View menu, select System Status, and then select a new or existing window. Expand the ILS wireless panel icon to show the locks assigned to it.

2. In the system status tree, complete either of the following steps:
   a. Right-click on an ILS Wireless panel icon, select Reader Access Modes, and then the access mode for all locks assigned to that panel.
   b. (Optional) Right-click on an individual ILS wireless lock icon, select Reader Access Modes, and then the access mode for that lock, exclusively. When the Reader Access Modes command is successfully issued, the request is queued up at the Wireless Gateway waiting for the next heartbeat.
   c. (Optional) You can also change the reader access mode of all locks from a reader device group. For more information, refer to Reader Group Right-click Options on page 146. For adding an ILS wireless lock to a reader device group, refer to the System Administration User Guide.

   - Select Device Groups from the View menu. The Device Groups window displays the currently configured device groups within a monitoring zone. The Device Groups window allows you to view and change the status of reader devices.
   - Expand the Device Groups icon.
   - Right-click on the reader device group icon, and then select Reader Access Modes, and then the access mode for all locks in the group.
Secure/Unsecure All Locks from a Reader Device Group

In emergency situations, use the Secure All or Unsecure All command to lock or unlock all ILS wireless locks assigned to a reader device group. For more information, refer to Adding a Device Group in the System Administration User Guide and Access Control Procedures Checklist on page 50.

From Alarm Monitoring, complete the following steps:

1. Select Device Groups from the View menu. The Device Groups window displays the currently configured device groups within a monitoring zone. The Device Groups window allows you to view and change the status of reader devices.
2. Expand the Device Groups icon.
3. Right-click on the reader device group icon, and then select Secure All. All ILS wireless locks in the reader device group are locked and set to the secured mode.
4. (Optional) Right-click on the device group icon, and then select Unsecure All. All ILS wireless locks in the reader device group are unlocked and set to the unsecured mode.

Wireless Diagnostics Dialog

From/To

The time range for which the wireless diagnostics data is available for the lock.

- From: mm/dd/yyyy hh:mm:ss AM/PM
- To: mm/dd/yyyy hh:mm:ss AM/PM

Signal Strength

This is the relative signal strength being received by the antenna for unlink/downlink communication. Signal strength values range from 0 - 3 with the higher values indicating a stronger signal.

Packet success rate (%)

This is the average success rate of transferred packets for unlink/downlink communication. 100% indicates that all packets were transferred successfully (no loss).
Retries per 100 packets
This the average number of retry attempts per 100 packets for unlink/downlink communication. A value of zero (0) indicates no packets were retried. Values greater than zero (0) indicate that retries were attempted. Less retries is desirable.

Reset
Clears all diagnostic data stored for the lock.

Refresh
Updates the diagnostic information for the lock.

Close
Closes the Wireless Diagnostics dialog.

View Wireless Diagnostics Information
During each heartbeat, uplink/downlink communication data is stored for the ILS wireless lock. Uplink refers to the signal sent from the Wireless Gateway whereas downlink is the signal received by the lock. This information is used to calculate the wireless diagnostics from Alarm Monitoring to check the health of the wireless network.

The data is stored for a specified number of days. When the data is older than the specified days, the system automatically purges the lock’s diagnostic information. For more information, refer to ILS System Options in the System Administration User Guide.

From Alarm Monitoring, complete the following steps:

1. Open the System Status Tree:
   a. From the View menu, select System Status, and then select a new or existing window.
   b. Expand the ILS wireless panel icon to show the locks assigned to it.

2. Right-click on the ILS wireless lock, and then select View Wireless Diagnostics. The Wireless Diagnostics dialog is displayed for the lock.

ILS Wireless Firmware

IMPORTANT: It is recommended to use the most current version of the firmware.

The Wireless Gateway contains two (2) micro-controllers:
- Wireless WAP Module (WWM)
- WAP Main Controller (WMC)

ILS wireless locks have 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 can be downloaded from Alarm Monitoring.

Note: Reader firmware is not available for magnetic type locks.
Download Wireless Gateway Firmware

From Alarm Monitoring, complete the following steps:

1. Open the System Status Tree. From the View menu, select System Status, and then select a new or existing window.
2. Right-click on the Wireless Gateway panel you want to upgrade, and then select Download Firmware > Wireless Gateway. The panel status shows the updated firmware version for the WWM and WMC when the download is completed successfully.

Download ILS Wireless Lock Firmware

In Alarm Monitoring, complete the following steps:

1. Open the System Status Tree.
   a. From the View menu, select System Status, and then select a new or existing window.
   b. Expand the Wireless Gateway panel icon to show the locks assigned to it.
2. Upgrade the firmware of all locks assigned to a Wireless Gateway. Right-click on the Wireless Gateway, and then select Download Firmware > ACU, WLM, or Reader.
3. (Optional) Upgrade the firmware of individual wireless locks. Right-click on the lock you want to upgrade, and then select Download Firmware > ACU, WLM, or Reader.

During the lock firmware download operation, the device status reports the progress:

- “Firmware download pending” is displayed when the request is queued up at the Wireless Gateway while the system waits for the next lock heartbeat.
- “Downloading firmware” is displayed when the locks receive the Download Firmware command from the Wireless Gateway and the download operation is started.
- When the firmware download is complete, the displayed firmware versions are updated and the Main Alarm Monitor window shows the firmware upgraded events.
Index

A
Access levels
  assign to a badge ............................... 213
  assign to cardholder group .................. 216
Access Levels form (Cardholders folder) .. 211
  procedures ......................................... 213
Accounts ............................................. 23
Acknowledge an alarm .......................... 159
Action Group Properties window .............. 352
Action History/Guard Tour Event Purging
  Properties window .................................. 354
Actions .............................................. 349
Activate single or double left-click mode  149
Activation dates assign .......................... 214
Active visits ......................................... 246
Add
  action group ....................................... 353
  action history/guard tour event purging
    action ........................................... 355
  archive/purge database action .............. 356
  arm/disarm area action ........................... 358
  asset .............................................. 276
  asset groups and classes ..................... 282
  asset type/subtype ............................. 277
  automatic guard tour action .................. 360
  cardholder record .................................. 197
  columns .......................................... 58
  deactivate badge action ........................ 364
  device output action ............................ 365
  device output group action ..................... 367
  elevator mode action ........................... 372
  elevator terminal allowed floors action .... 368
  elevator terminal mode action ................ 369
  execute function list action .................. 371
global APB system/segment reset
  action ............................................. 373
ISC database download action ................ 375
ISC firmware download action ................ 376
mask/unmask alarm input action .............. 380
mask/unmask alarm input for group
  action ............................................. 382
mask/unmask alarm mask group
  action ............................................. 383
mask/unmask door action ..................... 385
mask/unmask door forced open action .......... 386
mask/unmask door forced open for reader
  group action ..................................... 388
mask/unmask door held open action ............ 390
mask/unmask door held open for reader
  group action ..................................... 391
muster mode initiation action ............... 379
pulse open door action .......................... 393
pulse open door group action ............ 394
reader mode action ................................ 396
reader mode group action ....................... 398
readers ............................................. 137
report ............................................... 294
reset use limit action ........................... 400
run PTZ tour action ............................... 401
schedule report action ........................... 403
set forwarding station action ................. 409
sign out visitor action .......................... 410
silence area action ................................ 412
visit record ........................................ 248
visitor record ..................................... 200
Add Recipient window ............................. 260
Alarm
  icons .............................................. 151
  overview .......................................... 46
pending alarms ........................................... 152
Alarm Acknowledgment Reports form .......... 313
Alarm descriptions .................................... 413
Alarm Monitoring Operator Procedures ........ 51
Alarm Monitoring overview ....................... 21
Alarm Monitoring window ......................... 169
Alarm Panel Reports form ......................... 299
procedures ............................................... 301
Alarms - Muster mode ................................ 169
Anti-Passback Reports form ....................... 302
procedures ............................................... 305
Archive/Purge Database Properties window .... 355
Arm ........................................................ 357
Arm/Disarm Area Properties window .......... 356
Arrange columns ....................................... 58
Asset classes
add .......................................................... 281
Asset Classes form ..................................... 278
procedures ............................................... 281
Asset groups
add .......................................................... 281
Asset menu ............................................... 45
Assets
assign to cardholder ................................... 225
Assets form
Cardholders folder ..................................... 224
procedures ............................................... 225
Assets form (Assets folder) ......................... 272
procedures ............................................... 275
Assign
cardholder to an asset ................................ 285
classes to an asset .................................... 281
Assign Intrusion Authority to the Cardholder ... 214
Assignments form ...................................... 283
procedures ............................................... 285
Authenticating video files ......................... 511
setting a watermark ................................... 511
Automatic Guard Tour respond to ................ 334
schedule ............................................... 333
Automatic Guard Tour Properties window ..... 358

B
Badge form ............................................... 203
procedures ............................................... 208
Badges
add or replace record ............................... 208
assign access levels .................................. 213
assign precision access group .................. 220
encode .................................................... 211
move all ............................................... 172
move one ............................................... 173
Barcodes
CAC .......................................................... 185
configuring to read CAC barcodes ............. 185
scanning with a wedge scanner ............... 185
Biometrics
search records ......................................... 222
Biometrics form
Cardholders folder ................................... 221
procedures ............................................... 222
Buffering Video ........................................ 82

C
CAC barcodes ............................................ 185
Camera lookup ....................................... 83
Cameras (surveillance-only) ....................... 87
Capture an image ..................................... 113
Cardholder form ...................................... 192
procedures ............................................... 197
Cardholder menu - bulk sub-menu ............. 43
Cardholders
assign access levels to cardholder group .......... 216
destroy all data ....................................... 198
modify segment assignments .................... 202
retrieve recent search results ................... 183
run reports ............................................. 229
search for cardholders ............................. 182
Cardholders folder .................................. 177
Access Levels form ................................... 211
ILS Authorization form ............................. 231
procedures ............................................... 181
Change Network Video Password Properties window ........................................... 360
Checkpoint status and events diagram .......... 335
Checkpoint time ....................................... 329
Checkpoints .......................................... 329
Client Side Caching ................................... 82
Comparison operators ................................ 181, 245
Configure
wedge scanner ....................................... 188
Configure menu ....................................... 36
Control menu ........................................... 36
Control menu - “current device” sub-menu .... 37
Conventions used in this documentation ....... 21
Convert and export video ......................... 510
Create a video event .................................. 113
Create custom video tour ......................... 80
Customize Overlay Information Dialog ....... 508

D
Date/Time Reports form ............................. 306
procedures ............................................... 309
Deactivate Badge Properties window .......... 363
Deactivation dates assign ......................... 214
De-interlacing ........................................... 111
Delete
alarm ...................................................... 161
alarm in standard Video Verification window .. 137
alarms (all) ............................................. 161
asset ...................................................... 276
badge record ........................................... 211
Index

Retrieve ILS Integra lock events ........................................ 516
ILS offline lock events .................................................... 516
ILS wireless firmware upgrades ........................................ 521
Images capture .................................................................. 113
Import
  cardholder data ......................................................... 193
  fingerprints from PIV card ........................................... 191
Initiate Muster mode ..................................................... 170
Instant arm ................................................................. 357
Interior ........................................................................... 357
Intrusion Detection Device Statuses .................................. 51
ISC Database Download Properties
  window ........................................................................... 374
ISC Firmware Download Properties
  window ........................................................................... 375

K
Keyboard Wedge Settings window ....................................... 184

L
Launch
  Guard Tour .................................................................... 332
Launch video
  direct from camera ......................................................... 86
  from archive server ......................................................... 86
  from failover recorder ..................................................... 86
  live ................................................................................. 86
  recorded ........................................................................... 86
Launch video from camera .................................................. 86
Left-click mode .................................................................. 149
Lenel ILS (Integrated Locking Solutions) .......................... 515
Lenel Video Export .......................................................... 506
Link
  cardholder to a directory account ..................................... 226
Linked maps ...................................................................... 162
Load a video file .............................................................. 112
Locate a device .................................................................. 71
Logging in
  using automatic single sign-on ......................................... 26
  using manual single sign-on ............................................. 27
  without using single sign-on ............................................ 24
Logging out of the application ............................................ 30
Lookup a cardholder assigned to an asset ......................... 285

M
Maps
  display ............................................................................ 161
  linked .............................................................................. 162
Mask/Unmask Alarm Input for Group
  Properties window .......................................................... 380
Mask/Unmask Alarm Input Properties
  window ........................................................................... 379
Mask/Unmask Alarm Mask Group Properties
  window ........................................................................... 382
Mask/Unmask Door Forced Open for Reader
  Group Properties window ................................................. 387
Mask/Unmask Door Forced Open Properties
  window ........................................................................... 385
Mask/Unmask Door Held Open for Reader
  Group Properties window ................................................. 390
Mask/Unmask Door Held Open Properties
  window ........................................................................... 388
Mask/Unmask Door Properties window ................................ 384
Master arm ................................................................. 357
Menus ............................................................................. 32
  asset menu .................................................................. 45
  cardholder menu .......................................................... 44
  bulk sub-menu ................................................................ 44
  configure menu ............................................................ 36
  control menu ............................................................... 36
  current device sub-menu ................................................. 37
  edit menu ..................................................................... 32
  file menu ..................................................................... 32
  help .............................................................................. 42
  options menu .............................................................. 39
  trace menu ................................................................... 35
  view menu ..................................................................... 33
  window ......................................................................... 42
Modify
  access levels assignments .............................................. 217
  asset ............................................................................. 276
  asset classes assignment ................................................. 281
  asset group ................................................................. 225
  badge record .................................................................. 209
  badges for selected cardholder group ............................. 209
  cardholder record ........................................................ 197
  cardholder’s permission to have visitors .......................... 223
  group of cardholder’s segments ...................................... 202
  report ............................................................................ 294
  scheduled action using the scheduler right-click menu ....... 345
  visit record ..................................................................... 251
  visitor record .............................................................. 200
Monitor (trace)
  individual devices .......................................................... 77
Monitor Devices ................................................................ 63
Monitor ILS wireless lock events ........................................ 517
Monitor video
  in matrix view ................................................................ 117
  with multiple cameras (successively) ............................... 113
  with one specific camera ................................................. 87
Move
  all badges ..................................................................... 172
  one badge .................................................................... 173
Multiple hardware views - display ....................................... 59
Muster mode
  alarm ............................................................................ 169
  initiate ........................................................................ 170
  reports .......................................................................... 171, 172
  reset ............................................................................. 171
Muster mode report ............................................................ 171

O
Occupancy report ............................................................. 171
Offline locks
S

Scan barcodes with wedge scanner .......... 185
Schedule
  action ................................................... 338
  automatic Guard Tour action .......... 333
  one-time password change ............... 362
  recurring password change ............. 362
  visits .................................................. 246
Schedule Report Properties window .......... 401
Scheduler folder .................................. 337
Scheduler form (Scheduler folder) ........... 337
  procedures ............................................. 338
  right-click menu .................................... 343
Search
  biometric records ................................ 222
  cardholder records .............................. 182
  comparison operators .......................... 181
  for a device ......................................... 71
  for all visits by a selected visitor ..... 246
  for all visits for a specific date or time 247
  for all visits to a selected cardholder 245
  for an asset record ............................... 277
  for devices ............................................ 71
  for scheduled, active, or finished visits 246
  report for specific information .......... 328
  video .................................................... 96
Search results
  retrieve recent search results .......... 183
Secure/Unsecure all locks in a reader device group ................................ 520
Security clearance levels
  assign .................................................. 228
Segmentation
  modify cardholder segment assignments . 202
Segments form
  Cardholders folder ............................ 201
  procedures .......................................... 202
Select
  column configuration ................................ 58
  events to monitor .................................. 57
  a device
    in single or double left-click mode .... 150
Select Date(s) window ........................ 255
Select Host Wizard-Search form ............ 263
Select Host Wizard-Select form ............ 264
Select Import Source window ............... 270
Select PTZ Preset Properties window ........ 405
Select Time Range window .................... 255
Select Visitor Wizard - Add form .......... 268
Select Visitor Wizard - Search form ........ 265
Select Visitor Wizard - Select form .......... 269
Select Visitor Wizard - Select or Add form 266
Send
  e-mail .................................................. 163
  page ................................................... 164
  video ................................................. 87
Sharpener .......................................... 111
Show Operator column ......................... 516

Sign in a previously scheduled visit ....... 252
Sign In Visit(s) window ....................... 242
Sign out a visit ................................. 253
Sign Out Visitor Properties window .......... 409
Signal strength .................................... 520
Single and double left-click mode .......... 149
Sort alarms ......................................... 153
Standard mode ..................................... 60
Standard video verification
  display cardholder photo and live video .................................................. 137
  remove readers ...................................... 137
Start an action ..................................... 343
Status bar - Alarm Monitoring window ....... 46
Status Search form ............................... 256
Stop an action ....................................... 343
Surveillance-only cameras .................... 87
Switch between camera and monitor views 119
Switch camera views in Video Player ........ 113
Switch log on .......................................... 29
System Hardware Options window .......... 55
System Status window ......................... 63, 170

T

Test a device ........................................... 70
Toolbars ................................................. 32
Trace Configuration window .................. 75
Trace Configuration Window Overview ...... 75
Trace menu ............................................. 35
Tree view .............................................. 61
Two-way audio ........................................ 84

U

Unassign an asset ..................................... 285
Unlink
  directory account ................................ 227
Update hardware status .......................... 70
User-defined display options .................. 55

V

Verify fingerprint ..................................... 191
Verify Fingerprint(s) Dialog .................... 190
Video
  create event ......................................... 113
  export ................................................ 509
  monitor ............................................. 113
  search ............................................... 96
  view search results ........................... 97
Video Channel Configuration
  configure parameters .......................... 98
  open dialog ......................................... 98
Video Channel Configuration dialog ........... 97
Video Export ......................................... 506
Video monitor features ........................... 82
Video monitoring features
  browser-based VideoViewer .................. 83
  Camera lookup ..................................... 83
  client side caching .............................. 82
### Index

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-way audio</td>
<td>84</td>
</tr>
<tr>
<td>Video monitoring procedures</td>
<td>86</td>
</tr>
<tr>
<td>Video Monitoring window</td>
<td>80</td>
</tr>
<tr>
<td>Video Player</td>
<td>105</td>
</tr>
<tr>
<td>switch camera views</td>
<td>113</td>
</tr>
<tr>
<td>Video quality enhancements</td>
<td>111</td>
</tr>
<tr>
<td>de-interlacing</td>
<td>111</td>
</tr>
<tr>
<td>fog removal</td>
<td>111</td>
</tr>
<tr>
<td>sharpener</td>
<td>107</td>
</tr>
<tr>
<td>status icon</td>
<td>107</td>
</tr>
<tr>
<td>Video Search window</td>
<td>88</td>
</tr>
<tr>
<td>Video Verification</td>
<td></td>
</tr>
<tr>
<td>digital video</td>
<td>134</td>
</tr>
<tr>
<td>standard CCTV</td>
<td>135</td>
</tr>
<tr>
<td>Video Verification window</td>
<td>133</td>
</tr>
<tr>
<td>VideoViewer (Browser-based)</td>
<td>83</td>
</tr>
<tr>
<td>View</td>
<td></td>
</tr>
<tr>
<td>action history</td>
<td>344</td>
</tr>
<tr>
<td>current status of an action</td>
<td>344</td>
</tr>
<tr>
<td>last connection time for dialup panels</td>
<td>71</td>
</tr>
<tr>
<td>linked maps</td>
<td>162</td>
</tr>
<tr>
<td>video files</td>
<td>112</td>
</tr>
<tr>
<td>video tour</td>
<td>81</td>
</tr>
<tr>
<td>View ILS wireless diagnostics information</td>
<td>521</td>
</tr>
<tr>
<td>View ILS wireless lock information</td>
<td>518</td>
</tr>
<tr>
<td>View menu</td>
<td>33</td>
</tr>
<tr>
<td>View offline lock events</td>
<td>516</td>
</tr>
<tr>
<td>View options change cardholders folder</td>
<td>183</td>
</tr>
<tr>
<td>view</td>
<td></td>
</tr>
<tr>
<td>Visit</td>
<td></td>
</tr>
<tr>
<td>right-click menu</td>
<td>240</td>
</tr>
<tr>
<td>search capabilities</td>
<td>244</td>
</tr>
<tr>
<td>Visit form</td>
<td>254</td>
</tr>
<tr>
<td>Visit search results</td>
<td>248</td>
</tr>
<tr>
<td>Visitor</td>
<td></td>
</tr>
<tr>
<td>add record</td>
<td>200</td>
</tr>
<tr>
<td>find cardholder/visitor associated with a visit</td>
<td>248</td>
</tr>
<tr>
<td>print badge for a visitor</td>
<td>252</td>
</tr>
<tr>
<td>search for all visits by a selected visitor</td>
<td>246</td>
</tr>
<tr>
<td>Visitor form</td>
<td>199</td>
</tr>
<tr>
<td>procedures</td>
<td>199</td>
</tr>
<tr>
<td>Visits</td>
<td></td>
</tr>
<tr>
<td>active</td>
<td>246</td>
</tr>
<tr>
<td>add a visit record</td>
<td>248</td>
</tr>
<tr>
<td>delete a visit record</td>
<td>252</td>
</tr>
<tr>
<td>find cardholder/visitor associated with a visit</td>
<td>248</td>
</tr>
<tr>
<td>finished</td>
<td>246</td>
</tr>
<tr>
<td>modify a visit record</td>
<td>251</td>
</tr>
<tr>
<td>retrieve recent search results</td>
<td>183</td>
</tr>
<tr>
<td>retrieve recent visit search results</td>
<td>248</td>
</tr>
<tr>
<td>run a visit report from the Visits folder</td>
<td>262</td>
</tr>
<tr>
<td>search all visits by selected visitor</td>
<td>246</td>
</tr>
<tr>
<td>search all visits for specific date or time</td>
<td>247</td>
</tr>
<tr>
<td>search all visits to selected cardholder</td>
<td>245</td>
</tr>
<tr>
<td>search for active visits</td>
<td>246</td>
</tr>
<tr>
<td>search for finished visits</td>
<td>246</td>
</tr>
<tr>
<td>search for scheduled visits</td>
<td>246</td>
</tr>
<tr>
<td>sign in a previously scheduled visit</td>
<td></td>
</tr>
<tr>
<td>sign out a visit</td>
<td>253</td>
</tr>
<tr>
<td>Visits folder</td>
<td></td>
</tr>
<tr>
<td>field table</td>
<td>241</td>
</tr>
<tr>
<td>procedures</td>
<td>244</td>
</tr>
<tr>
<td>Visits form</td>
<td></td>
</tr>
<tr>
<td>Cardholders folder</td>
<td>222</td>
</tr>
<tr>
<td>procedures</td>
<td>223</td>
</tr>
</tbody>
</table>

### W

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watermarking</td>
<td>511</td>
</tr>
<tr>
<td>authentication</td>
<td>512</td>
</tr>
<tr>
<td>Weak database password warning</td>
<td>23</td>
</tr>
<tr>
<td>Wedge scanner</td>
<td></td>
</tr>
<tr>
<td>add a badge</td>
<td>184</td>
</tr>
<tr>
<td>configure</td>
<td>188</td>
</tr>
<tr>
<td>scanning barcodes</td>
<td>185</td>
</tr>
<tr>
<td>search for a badge</td>
<td>184</td>
</tr>
<tr>
<td>Wedge Settings window</td>
<td>184</td>
</tr>
<tr>
<td>Window display modes</td>
<td>59</td>
</tr>
<tr>
<td>floating</td>
<td>60</td>
</tr>
<tr>
<td>standard</td>
<td>60</td>
</tr>
<tr>
<td>Window menu</td>
<td>42</td>
</tr>
<tr>
<td>Wireless Diagnostics dialog</td>
<td>520</td>
</tr>
<tr>
<td>Wireless lock</td>
<td></td>
</tr>
<tr>
<td>packet retries</td>
<td>521</td>
</tr>
<tr>
<td>packet success rate</td>
<td>520</td>
</tr>
<tr>
<td>Signal strength</td>
<td>520</td>
</tr>
<tr>
<td>Wizards</td>
<td></td>
</tr>
<tr>
<td>select host wizard (Search form)</td>
<td>263</td>
</tr>
<tr>
<td>select host wizard (select form)</td>
<td>264</td>
</tr>
<tr>
<td>select visitor wizard (Add form)</td>
<td>268</td>
</tr>
<tr>
<td>select visitor wizard (select or add form)</td>
<td>266</td>
</tr>
</tbody>
</table>

529 Alarm Monitoring User Guide