AVIGILON™

# Admin Guide

Access Control Manager™

Version 6.50.0

© 2016 - 2024, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logos, AVIGILON CONTROL CENTER, ACC, ACCESS CONTROL MANAGER, ACM and ACM VERIFY are trademarks of Avigilon Corporation. Digital Monitoring Products® is a registered trademark of Digital Monitoring Products. Remote Link is a trademark of Digital Monitoring Products, Incorporated. HID, HID GLOBAL, HID Mercury, HID Mobile Access, APERIO and VERTX are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries. Allegion, ENGAGE technology and Schlage are trademarks of Allegion plc, its subsidiaries and/or affiliates in the United States and other countries. Linux is a registered trademark of Linus Torvald in the US and other countries. Firefox is a trademark of the Mozilla Foundation in the US and other countries. Microsoft and SQL Server are trademarks of the Microsoft group of companies. Other names or logos mentioned herein may be the trademarks of their respective owners. The absence of the symbols ™ and ® in proximity to each trademark in this document or at all is not a disclaimer of ownership of the related trademark.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
avigilon.com

PDF-ACM-ADM-6.50.0-A

Revision: 1 - EN

20240121

# Revisions

| ACM Release | Description |
| --- | --- |
| ACM 6.50.0 | Re-trust SSL certificates after upgrading to ACM 6.50:<br>• *Re-trust Certificates* on page 398<br>• *System Settings - External Domains list* on page 399<br>• *Managing Collaborations* on page 362<br>Performance improvements for large scale environments and other enhancements and corrections:<br>• *Adding Holidays* on page 379<br>• *Adding a License* on page 357<br>• *Step 2: Setting Up Communication to Offline Wi-Fi Locks* on page 277<br>• *System Settings - Certificates list* on page 402<br>• *Supported Collaborations* on page 369 |

# Table of Contents


Revisions ... 3

Introduction ... 21
- Logging In ... 21
- Managing Notes ... 22

Initial Setup ... 23
- Accepting the End User License Agreement ... 23
- Upgrading Your License Format ... 23
- Adding a License ... 24
  - Online Licensing ... 24
  - Offline Licensing ... 24
- Changing the Administrator Password ... 25
- Creating a Super Admin Identity ... 25

Monitoring ... 26
- Monitoring Events ... 26
  - Pause/Resume Events ... 27
  - Clear Events ... 27
  - View Live Video ... 27
  - View Recorded Video ... 28
  - Create Event Notes ... 28
  - View Event Notes ... 28
  - View Event Instructions ... 29
  - View Event Identity Details ... 29
  - View Event History ... 29
  - Change Events List Settings ... 30
  - Reconnect to Events List ... 30
- Searching for Events and Alarms ... 30
  - View Camera (Search) ... 31
  - View Recorded Video (Search) ... 31
  - Create Event Notes (Search) ... 32
  - View Event Notes (Search) ... 32
  - View Event Instructions (Search) ... 33
  - View Event Identity Details (Search) ... 33
  - View Event History (Search) ... 33
  - Change Transactions List Settings ... 33
- Monitoring Alarms ... 34
  - Acknowledge Alarms ... 35
  - Assign Alarms ... 35
  - View Live Video (Alarms) ... 36
  - View Recorded Video (Alarms) ... 36
  - Create Event Notes (Alarms) ... 36

View Event Notes (Alarms) ..... 37
View Event Instructions (Alarms) ..... 37
View Event Identity Details (Alarms) ..... 38
View Event History (Alarms) ..... 38
Change Alarms List Settings ..... 38
Turning Sound On/Off ..... 39
Using the Verification page ..... 39
Verifying Identities at Doors ..... 39
Verification Events List ..... 40
Using the Dashboard ..... 41
Status Colors ..... 43
Appliance Transactions Indicators ..... 43
Device Status ..... 43
Security Status ..... 44
Installing, Uninstalling and Deleting Panels and Subpanels ..... 45
Viewing, Masking and Unmasking Inputs ..... 45
Viewing, Activating and Deactivating Outputs ..... 45
Searching Panel, Subpanel, Input and Door Names ..... 45
Saving Door Filters ..... 46
Controlling Doors ..... 46
Accessing Web Interface of Power Panels ..... 47
Using Map Templates ..... 47
Using a Map ..... 48
Viewing a Map ..... 48
Hardware Status ..... 49
Map Actions ..... 49
Adding Maps ..... 52
Monitoring Bosch Intrusion Panels ..... 52
Monitor Bosch Intrusion Panel Status ..... 52
Monitoring Areas in Bosch Intrusion Systems ..... 53
Viewing Areas ..... 53
Arming Areas ..... 54
Arming Perimeter Areas ..... 54
Disarming Areas ..... 54
Silencing Keypad Alarms ..... 54
Clearing Alarms ..... 54
Resetting Sensors ..... 54
Monitor Bosch Intrusion Panel Points ..... 54
Monitor Bosch Intrusion Panel Outputs ..... 55
Monitoring and Controlling DMP Intrusion Systems ..... 56
Viewing Panels, Areas, Zones and Outputs ..... 56
Silencing Keypad Alarms on Panels ..... 57

Resetting Sensors on Panels ... 57
Arming or Disarming Areas ... 58
Bypassing Zones and Resetting Bypassed Zones ... 58
Activating and Deactivating Outputs ... 58

Identities ... 60
Setting Up Multi-Factor Authentication ... 60
Add Your MFA Devices ... 60
Add MFA Device ... 60
Delete MFA Device ... 61
Disable MFA ... 61
Configuring HID Mobile Access® Credentials ... 62
Prerequisites ... 62
Step 1: Connecting to the HID Origo External System ... 62
Step 2: Enrolling Identities and Issuing Tokens ... 63
Issuing a Token to an Enrolled Identity on a Registered Mobile Device ... 63
Registering a New Mobile Device for an Enrolled Identity ... 64
Searching for HID Origo Tokens ... 64
Searching for an Identity ... 64
Adding an Identity ... 65
Assigning Roles to Identities ... 66
Assigning Tokens to Identities ... 67
Assigning Groups to Identities ... 67
Deleting a Token ... 68
Capturing and Uploading Photos of an Identity ... 68
Creating Badges for Identities ... 72
Timed Access ... 73
Adding Timed Access to an Identity ... 74
Editing Timed Access ... 75
Deleting Timed Access ... 75
Editing an Identity ... 75
Token Fields ... 76

Managing Roles ... 82
Configuring Roles ... 82
Adding a Role ... 82
Editing a Role ... 83
Assigning an Access Group to a Role ... 83
Assigning Delegations to a Role ... 84
Assigning Routing Groups to a Role ... 84
Assigning Roles ... 85
Deleting a Role ... 85
Searching for Roles ... 85
Role Fields ... 86

Roles - Access Groups page ..... 87
Roles - Delegate page ..... 88
Roles - Routing page ..... 88
Roles - Assign Roles page ..... 89
Roles - Access page ..... 89
Roles - Audit page ..... 90
Configuring Policies ..... 90
Adding a Policy ..... 90
Editing a Policy ..... 91
Deleting a Policy ..... 91
Policies list ..... 91
Policies - Policy Add page ..... 92
Policies - Policy: Add page ..... 92
Policies - Mercury Security page ..... 93
Policies - Input page ..... 96
Policies - Output page ..... 97
Policies - Audit page ..... 97
Configuring Groups ..... 98
Adding a Group ..... 98
Editing a Group ..... 98
Assigning Policies to Groups ..... 99
Assigning Members to Groups ..... 99
Creating a Hardware Group for Routing ..... 100
Using Policies to Override Hardware Settings ..... 100
Performing an Identity Batch Update ..... 101
Performing a Batch Update from the Identity Profiles page ..... 101
Performing a Batch Update from the Groups page ..... 101
Performing an Identity or Template Batch Update ..... 101
Scheduling an Identity or Door Batch Update ..... 102
Deleting a Group ..... 103
Groups list ..... 103
Groups - Group Add page ..... 103
Groups - Group Edit page ..... 103
Groups - Policies page ..... 103
Groups - Members page ..... 104
Groups - Audit page ..... 104
Managing Door Access ..... 105
Adding an Access Group ..... 105
Editing an Access Group ..... 106
Deleting an Access Group ..... 106
Access Groups - Example ..... 107
Assigning an Access Group to a Role ..... 107

Searching for Access Groups ..... 108
Access Group Fields ..... 109
Access Groups - Access page ..... 109
Access Groups - Audit page ..... 110
Managing Access in the Application ..... 110
Adding a Delegation ..... 110
Editing a Delegation ..... 111
Adding a Delegation to a Role ..... 111
Deleting a Delegation ..... 112
Delegations list ..... 112
Delegations - Delegation: Edit page ..... 112
Managing a Partitioned ACM System ..... 113
Planning a Partitioned System ..... 114
Configuring a Partitioned ACM System ..... 115
Adding a Partition ..... 116
Editing a Partition ..... 116
Deleting a Partition ..... 117
Partitions - List ..... 117
Partitions - Add page ..... 117
Partitions - Partition Edit page ..... 118
Assigning Partitions to ACM Operators and Entities ..... 118
Routing Events to the Monitor Screen ..... 119
Routing Groups - Introduction ..... 119
Adding a Routing Group ..... 120
Editing a Routing Group ..... 120
Assigning a Routing Group to a Role ..... 121
Deleting a Routing Group ..... 121
Routing Groups list ..... 121
Routing Groups - Add page ..... 122
Routing Groups - Schedule page ..... 122
Routing Groups - Event Types page ..... 123
Routing Groups - Groups page ..... 123
Managing Elevator Access ..... 124
Adding an Elevator Access Level ..... 124
Editing an Elevator Access Level ..... 124
Assigning an Elevator Access Level to an Access Group ..... 124
Deleting an Elevator Access Level ..... 125
Elevator Access Levels list ..... 125
Elevator Access Levels - Add page ..... 125
Elevator Access Levels - Elevator Access Level: Edit page ..... 126
Reports ..... 127
Generating Reports ..... 127

Report Preview ..... 127
Editing Reports ..... 128
Editing Audit Log and Transaction Reports ..... 129
Creating Custom Reports ..... 130
Scheduling a Custom Report By Batch Job (Specification) ..... 130
Creating Custom Audit Log and Transaction Reports ..... 131

Physical Access ..... 133
Templates Overview ..... 133
Door Templates ..... 134
Door Templates - Batch Update ..... 134
Door Templates list page ..... 135
Door Templates - Add page ..... 135
Door Templates - Door Template: Edit page ..... 137
Door Templates - Batch Update ..... 139
Reader Templates ..... 140
Reader Templates list page ..... 140
Reader Template: Add page ..... 140
Reader Template: Edit page ..... 143
Input Templates ..... 146
Input Templates list page ..... 146
Input Template: Add page ..... 147
Input Template: Edit page ..... 148
Output Templates ..... 150
Output Templates list page ..... 150
Output Template: Add page ..... 150
Output Template: Edit page ..... 151
Wiring Templates ..... 152
Wiring Templates list page ..... 153
Wiring Template: Add page ..... 153
Wiring Template: Edit page ..... 155
Configuring Panels ..... 155
Searching for Panels ..... 156
Panel Migration ..... 156
HID VertX V1000 to Mercury Security LP4502 ..... 156
Mercury Security EP to LP Panel ..... 158
Adding Panels ..... 158
Configuring the Mercury Security MS Bridge Solution ..... 161
Batch Creating Subpanels on a New Mercury Panel ..... 161
Subpanel: Batch Create page ..... 163
Subpanel: Batch Edit Details page ..... 163
Subpanel: Batch Name Doors or Subpanel: Batch Create Summary page ..... 164
Adding HID VertX® Subpanels ..... 164

Adding Mercury Security Panels ....164
Subpanel Fields ....165
Subpanel: Batch Add page (VertX®) ....166
Editing Panels ....166
Editing HID® VertX® Panels ....166
Editing Mercury Security Panels ....166
167
Panel Card Formats ....167
ENGAGE Gateway Configuration ....167
SALTO Panel Status ....168
SALTO Panel Configuration ....168
ASSA ABLOY Panel Configuration ....168
Resetting Anti-Passback from the Panel ....169
Downloading Parameters ....169
Downloading Tokens ....169
Lenel Panel Support ....169
Resetting Doors Connected to a Subpanel ....170
Updating Panel Firmware ....170
Updating Schlage Gateway Firmware ....171
Updating Panel Time ....172
Deleting Panels ....172
Configuring Subpanels ....172
Adding a Subpanel ....173
Editing Subpanels ....174
Inputs ....175
Output Operating Modes ....175
Outputs ....176
Deleting Subpanels ....176
Configuring Locks ....176
Supported Devices ....177
Configuring ASSA ABLOY™ Aperio® Wireless Lock Technology ....178
Configuring Allegion Schlage AD-400 Series Locks ....179
Configuring Allegion Schlage LE Series Locks ....180
Configuring Allegion Schlage NDE Series Locks ....181
Configuring SimonsVoss Wireless Locks ....183
Prerequisites ....183
Configuring Doors ....184
Troubleshooting ....186
Door Is Not Online ....186
Door Status ....186
Macros ....186
Adding Macros ....187
Editing Macros ....187

Deleting Macros ..... 188
Assigning Macros ..... 188
Assigning a Macro to a Trigger ..... 188
Assigning a Macro to a Macro ..... 188
Assigning a Macro to a Door ..... 188
Sorting Macros ..... 188
Triggers ..... 189
Adding Triggers ..... 189
Editing Triggers ..... 189
Deleting Triggers ..... 189
Configuring Doors ..... 189
Searching for Doors ..... 190
Advanced Filtering on the Doors List ..... 191
Controlling Doors ..... 191
Configuring Door Held-Open Settings ..... 192
Adding Doors ..... 193
Adding Simple Macros ..... 200
Editing Doors ..... 201
Doors - Editing VertX® Doors ..... 202
Doors - Editing Mercury Security Doors ..... 202
Deleting Doors ..... 202
Door Modes ..... 203
Access Types ..... 204
Anti-Passback ..... 205
Anti-Passback Modes ..... 205
Setting Up Anti-Passback ..... 207
Two-Person Minimum Occupancy and Single Door Configuration ..... 208
Granting a Free Pass ..... 210
Global Anti-Passback ..... 210
Global Anti-Passback Modes ..... 210
Interlocks ..... 210
Adding Interlocks ..... 211
Editing Interlocks ..... 212
Doors list ..... 212
Adding Doors ..... 214
Doors - VertX® New Parameters page ..... 221
Doors - Mercury Security New Parameters page ..... 223
Doors - Door: Edit Screen ..... 226
Door: Edit page (VertX® ) ..... 227
Parameters tab (VertX® ) ..... 227
Operations tab (VertX®) ..... 229
Hardware tab (VertX®) ..... 231
Reader Edit page (VertX®) ..... 232

Input Edit page (VertX®) 233
Output Edit page (VertX®) 234
Cameras tab (VertX®) 234
Events tab 236
Doors - Creating Local Events for VertX® Doors 237
Access tab (VertX® ) 238
Transactions tab (VertX® ) 239
Door: Edit page (Mercury Security) 239
Parameters tab (Mercury Security) 239
Operations tab (Mercury Security) 243
Hardware tab (Mercury Security) 246
Reader Edit page (Mercury Security) 248
Input Edit page (Mercury Security) 250
Output Edit page (Mercury Security) 251
Elev tab (Mercury Security) 251
Cameras tab (Mercury Security) 251
Configuring and Viewing Live Video Stream 253
Overview 253
Configuring Live Video Stream 254
Interlocks tab (Mercury Security Doors) 254
Interlocks Add page 254
Interlock Edit page 255
Events tab 256
Doors - Creating Local Events for Mercury Security Doors 257
Access tab (Mercury Security) 259
Transactions tab (Mercury Security) 259
Doors - Access page 259
Viewing Door Events, Access Groups and Transactions 260
Configuring ACM Verify™ Virtual Doors 261
Adding an ACM Verify Door 261
Parameters tab (Avigilon) 262
Paired Devices 263
Prerequisites for Pairing Devices 263
Precautions for Paired ACM Verify Stations 264
Pairing a Device 264
Using ACM Verify 265
IP/PoE Mode Installation 266
System Overview 266
Supported Devices 266
Step 1: Creating an ENGAGE Site 267
Step 2: Configuring Gateways for IP-enabled Wireless Locks 268
Step 3: Configuring IP-enabled Wireless Devices 269
Step 4: Configuring Locking Operation 270
Applying Door Commands 271
Door Scheduling By Batch Job (Specification) 272
Viewing Gateway or Offline Wi-Fi Lock Status 272

Viewing Door Status and Events ... 273
Updating Gateway and Offline Wi-Fi Lock Firmware ... 274
Generating Reports ... 275
Offline Wi-Fi Mode Installation ... 275
Supported Devices ... 276
Step 1: Creating an ENGAGE Site ... 276
Step 2: Setting Up Communication to Offline Wi-Fi Locks ... 277
Step 3: Configuring Offline Wi-Fi Lock Operation ... 278
Viewing Gateway or Offline Wi-Fi Lock Status ... 279
Updating Lock Firmware ... 279
Deleting Offline Wi-Fi Locks ... 280
SALTO Door Installation ... 281
System Overview ... 281
Prerequisites ... 282
SALTO Server Installation and Configuration ... 282
Understanding SALTO and ACM Door Configuration ... 283
Escape and Return Mode ... 284
SALTO Ethernet Encoder Configuration ... 285
Supported Devices ... 285
Step 1: Connecting to a SALTO Server ... 285
Step 2: Configuring the SALTO Server ... 286
Step 3: Syncing Doors with the SALTO Server ... 286
Step 4: Installing and Configuring Doors ... 287
Step 5: Creating Identities and Tokens ... 288
Using Physical and Mobile Keys ... 289
Editing Tokens — Update Required and Re-edition Required ... 290
Canceling Keys ... 291
Downloading All Tokens ... 292
ASSA ABLOY™ IP-enabled Lock Installation ... 293
System Overview ... 293
Prerequisites ... 294
Supported Devices ... 295
Step 1: Configuring a Door Service Router for IP-enabled Locks ... 295
Step 2: Syncing Doors with the Door Service Router ... 296
Step 3: Installing and Configuring Doors ... 297
Step 4: Configuring Locking Operation ... 298
Door Scheduling By Batch Job (Specification) ... 299
Configuring Areas ... 299
Searching for an Area ... 300
Adding Areas ... 301
Editing Areas ... 301
Deleting Areas ... 301

EOL Resistance ..... 301
Adding EOL Resistance for Mercury Input Points ..... 302
Adding EOL Resistance for VertX® Input Points ..... 302
Editing EOL Resistance for Mercury Input Points ..... 302
Editing EOL Resistance for VertX® Input Points ..... 302
Mercury LED Modes - List page ..... 302
Editing LED Modes ..... 303
Restoring to Default States ..... 303
Mercury Security LED Mode Table page ..... 304
LED Modes for Mercury Security ..... 304
Configuring Card Formats ..... 305
Supported Card Formats ..... 305
Corporate Card Mode for Using Facility Codes ..... 306
Issue Level Numbering for Reusing a Card Number ..... 307
Adding Card Formats ..... 308
Editing Card Formats ..... 308
Deleting Card Formats ..... 309
Card Format Fields ..... 309
Configuring ACM System Events ..... 312
Searching for ACM System Events ..... 312
Customizing ACM System Events ..... 312
Assigning Priority Colors to ACM System Events ..... 312
Global Actions ..... 314
Adding Global Actions ..... 315
Adding a Group of Global Actions ..... 315
Editing Global Actions ..... 315
Types of Global Actions ..... 315
Deleting Global Actions ..... 316
Creating Global Actions and Linkages for Bosch Intrusion System ..... 316
Intrusion panel alarm due to an event in the System ..... 316
Disable and enable doors from keypad ..... 317
Disarm Alarm on Access Grant with restricted authorities ..... 317
Creating Global Actions and Linkages for DMP Intrusion System ..... 317
Toggle Arming and Disarming Areas ..... 318
Searching for Global Actions ..... 318
Global Linkages - Introduction ..... 319
Searching for a Global Linkage ..... 319
Adding Global Linkages ..... 320
Editing Global Linkages ..... 320
Mustering ..... 320
Mustering - Requirements ..... 320
Mustering - Creating a Dashboard ..... 321

Mustering - Using the Dashboard ..... 322
Updating or Clearing the Area of an Identity ..... 323
Moving Identities between Areas ..... 323
Clear Identities from an Area ..... 324
Using Global Actions to Move or Clear Areas ..... 324

Managing Appliances ..... 326
Editing Appliance Settings ..... 326
Deleting an Appliance ..... 326
Configuring Replication and Failover ..... 327
Failover/Redundancy Feature ..... 327
Automatic failover ..... 328
Manual failover and failback ..... 328
Recommended System Architecture ..... 328
System Architecture for Replication ..... 328
System Architecture for Redundancy ..... 329
Replication and Failover Requirements ..... 331
1. Preparing Appliances for Replication and Failover ..... 332
Setting Up the Primary Appliance ..... 333
Setting Up Additional Appliances ..... 333
2. Setting Up Replication Between Appliances ..... 334
Enabling Replication on the Primary Appliance ..... 334
Enabling Replication on the Second Peer or Standby Appliance ..... 335
3. Adding a Replication Subscription ..... 336
Testing Replication ..... 339
Checking the Appliance Replication Status ..... 339
Testing Two-Way Replication ..... 341
4. Setting Up Failover ..... 342
Configuring Email Notifications for Replication Events ..... 344
Removing Replication and Failover ..... 345
Failing Over and Failing Back ..... 345
Automatic Failover ..... 346
Manual Failover ..... 346
Failback ..... 347
Monitoring Transactional Replication to Hot Standby ..... 348
Configuring Network Connections ..... 348
Configuring Ethernet Ports ..... 348
Adding Ethernet Routes ..... 349
Enabling Serial Ports ..... 349
Backups ..... 350
Backing Up System Data ..... 350
Manually Backing Up Data ..... 350
Restoring Backups ..... 351

Restoring Backups From Other Backup Events ..... 351
Logs ..... 353
Accessing Appliance Logs ..... 353
Software Updates ..... 353
Updating the Appliance Software ..... 353
SSL Certificates Overview ..... 354
Supported Certificate Standards ..... 355
Viewing the SSL Certificate ..... 355
Creating an SSL Certificate ..... 355
Creating a Certificate Signing Request ..... 356
Uploading an SSL Certificate ..... 357
About Appliances page ..... 357
Adding a License ..... 357
Online Licensing ..... 357
Offline Licensing ..... 358
Removing a License ..... 358
Online Licensing ..... 358
Offline Licensing ..... 359
Upgrading Your License Format ..... 360
Viewing the End User License Agreement ..... 360
About Appliances page ..... 360

Managing Collaborations ..... 362
Adding a Collaboration ..... 362
Adding an Events XML Collaboration ..... 363
Collaborations - Events XML Definitions ..... 364
Collaborations - Events XML Example ..... 367
Editing a Collaboration ..... 369
Supported Collaborations ..... 369
Running a Collaboration ..... 370
Previewing the General Identity Collaboration Log ..... 371
Extracting a CSV Zip File ..... 372
Deleting a Collaboration ..... 373
Assigning an Event Type to a Collaboration ..... 373

Setup & Settings ..... 375
Schedules and Holidays ..... 375
Schedules ..... 375
Holidays ..... 376
Searching for Schedules ..... 376
Adding Schedules (Intervals in Schedules) ..... 377
Editing Schedules ..... 378
Deleting Schedules ..... 378
Adding Holidays ..... 379

Editing Holidays ..... 380
Deleting Holidays ..... 380
Examples ..... 380
Example 1: Part-Day Holiday ..... 380
Example 2: Additional Access Time ..... 381
Event Types ..... 381
Adding Event Types ..... 384
Editing Event Types ..... 384
Deleting Event Types ..... 384
User Forms Overview ..... 385
Adding and Customizing Tabs with User Forms ..... 385
Assigning Tabs to Identities with User Forms ..... 386
Editing User Forms ..... 387
Deleting User Forms ..... 387
User Defined Fields ..... 387
Adding a Field for User Forms, Tabs and Lists ..... 387
Adding and Assigning Tabs to Identities with User Fields ..... 388
Adding User Defined Fields to Tabs ..... 389
User Defined Fields - Deleting Fields ..... 389
User Defined Tabs - Deleting ..... 389
User Lists ..... 389
Adding Items to a List ..... 390
User Lists - Editing Items ..... 390
User Lists - Deleting Items ..... 390
System Settings ..... 390
Remote Authentication - Introduction ..... 391
Configuring Remote Authentication Using SSL Certificates ..... 391
About Certificate Pinning ..... 392
Requirements for Using Pinned Certificates ..... 392
Requirements for Using Trusted Certificates ..... 392
Pinning or Trusting Certificates in the ACM System ..... 393
Enabling Remote Authentication for ACM Client Users ..... 394
System Settings - General Fields ..... 394
System Settings - Remote Authentication page ..... 397
Re-trust Certificates ..... 398
Re-trust certificates for external domains ..... 398
Re-trust certificates for identity LDAP pull collaborations ..... 399
Dismiss the warning banner ..... 399
System Settings - External Domains list ..... 399
System Settings - External Domains Add page ..... 400
System Settings - External Domain: Edit page ..... 401
System Settings - Certificates list ..... 402

Certificate Upload page ..... 402
Badge Templates and the Badge Designer ..... 403
Using the Badge Designer ..... 403
Badge Templates list ..... 408
External Systems ..... 409
Supported External Systems ..... 409
Adding External Systems ..... 410
Editing External Systems ..... 411
Editing an ENGAGE Site ..... 411
Deleting External Systems ..... 411
External Systems - Integrating an ACM Appliance into an ACC™ Site ..... 412
External Systems - Defining the Badge Camera for the System ..... 414
External Systems - ViRDI ..... 414
External Systems - ViRDI System Settings ..... 414
Bosch Intrusion Panels ..... 415
Integrating the ACM System with Bosch Intrusion Panels ..... 415
Adding a Bosch Intrusion Panel ..... 417
Editing a Bosch Intrusion Panel ..... 418
Viewing Auto-Synced Bosch Intrusion Panels ..... 418
Deleting a Bosch Intrusion Panel ..... 419
Viewing Bosch Intrusion Panel Areas ..... 419
Viewing Bosch Intrusion Panel Points ..... 419
Viewing Bosch Intrusion Panel Outputs ..... 419
Viewing Bosch Intrusion Panel Users ..... 420
Assigning Bosch Intrusion Panel Users to Identities ..... 420
Supported Bosch Intrusion Panels ..... 421
DMP Intrusion Panel Installation ..... 424
System Overview ..... 424
Prerequisites ..... 425
Remote Link Software Configuration ..... 425
A.C. Power Failure Notification ..... 426
Panel Encryption ..... 426
Remote Key ..... 426
Supported Devices ..... 426
Step 1: Connecting to a DMP Intrusion Panel ..... 426
Deleting a DMP Intrusion Panel ..... 427
Step 2: Viewing an Installed DMP Intrusion Panel and its Areas, Zones, Outputs and Users ..... 428
Step 3: Assigning DMP Intrusion Users to Identities ..... 428
Generating Reports ..... 428
Enabling Debug Logs ..... 428
Maps ..... 429
Creating a Map ..... 429
Editing a Map ..... 429

Configuring the Map Background ..... 430
Adding Items to the Map ..... 430
Setting the Icon Size ..... 431
Showing or Hiding Items ..... 431
Deleting Items ..... 431
Configuring the Mustering Dashboard Element ..... 431
Linking Maps ..... 432
Example Use ..... 432
Using a Map ..... 432
Viewing a Map ..... 432
Hardware Status ..... 433
Map Actions ..... 434
Assets ..... 436
Uploading Sound File ..... 436
Playing Sound Files ..... 437
Deleting Sound Files ..... 437
Assigning Sounds to Alarm Events ..... 437

Priority Situations ..... 438
Planning Priority Door Policies ..... 438
Priority Door Policies, Global Actions, and Modes ..... 439
Priority Door Policies and Emergencies ..... 440
Configuring a Secure High-Priority Emergency Response ..... 441
Testing a Secure Priority Emergency Response in the ACM System ..... 443
Activating the High-Priority Emergency Response ..... 443
During a High-Priority Situation ..... 444
Deactivating a Priority Door Policy ..... 445
Limitations of Priority Global Actions ..... 445
Priority Hierarchy ..... 446
Triggering Door Lockdown By Panic Button or Red Card ..... 447

Overriding Door Modes and Schedules ..... 450
Adding an Override ..... 450
Accessing the List of Overrides ..... 451
Monitoring Overrides ..... 452
Modifying and Deleting Overrides ..... 452
Modifying an Override ..... 453

Setting Personal Preferences ..... 455
Changing the Password in My Account ..... 455
Setting Your Preferred Language ..... 455
Scheduling Batch Jobs ..... 455
Generating a Batch Report ..... 456
Applying an Identity Profile to a Group Using a Job Specification ..... 457

Applying a Door Template to a Group Using a Job Specification ..... 458
Scheduling a Global Action ..... 460
Setting Batch Door Modes ..... 461

Permissions and Rights ..... 463
Permissions and Rights for MFA ..... 487
Permissions and Rights for Sound Assets ..... 488
Permissions and Rights for ACM Expedite Mobile App Users ..... 489

Troubleshooting ..... 490
Events ..... 490
Appliance Events ..... 490
Door Events ..... 490
Battery Level Events ..... 494
Control Lock Events ..... 495
RU and RM Device Events ..... 495
Intrusion Events ..... 496
DMP Intrusion Events ..... 496
DMP Intrusion Area ..... 496
DMP Intrusion Output ..... 496
DMP Intrusion Panel ..... 496
DMP Intrusion User ..... 498
DMP Intrusion Zone ..... 499
Panel Events ..... 500
SALTO Key Events ..... 501
Subpanel Events ..... 501
System Events ..... 501
Enabling Debug Logs ..... 502

Appendix: pivCLASS Configuration ..... 503
Overview ..... 503
Prerequisites ..... 503
Enabling FIPS 140-2 Encryption on ACM Appliances ..... 503
Enabling Large Encoded Card Format and Embedded Authorization on Panels ..... 504
Updating Firmware ..... 504
Adding Doors ..... 505
Adding Reader Templates ..... 505
Assigning Large Encoded Formats to Panels ..... 505
Viewing Identities and Tokens ..... 505
Monitoring Events ..... 506

Glossary ..... 507

# Introduction

This guide provides an overview of the Admin role as defined in the Avigilon Access Control Manager (ACM) software. This guide is meant to be used and referred to by those assigned the role of an Admin within the ACM software.

The Admin role oversees the ACM system. They are responsible for monitoring and maintaining the ACM system. For more information, see *Permissions and Rights* on page 463.

> **Note:** This guide does not define the role of an Admin on all sites. Please contact your System Administrator for more details.

## Logging In

You can log in to the ACM system from any web browser that has access to the same network.

1. Open your preferred browser.
2. In the address bar, enter the IP address of your ACM appliance.
3. Enter your username in the **Login** field.

   If enabled, enter also your remote login account in **Remote Login**. Enter the login name in this format: *username@domain.org*.
4. Enter your password in the **Password** field.
5. Click the **Sign in** button.

   If enabled, select the MFA device in **Device**. Enter the six-digit code generated by your authenticator app and click **Verify**.

   > **Note:** The MFA Device fields do not apply to Remote Login accounts.

   If prompted to change your password, enter the **Old Password** and new password in **Password**. Click **Save**.
6. The application's Home page is displayed.

   > **Note:** If you are logging in to the ACM application for the first time, the default password for the `admin` username must be changed. In addition, if you are performing a system upgrade, the default password for the admin username must be changed if it was not changed previously.

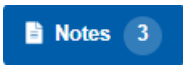
   > **Tip:** To change your password after initial installation, see *Changing the Password in My*

*Account* on page 455 and *Changing the Administrator Password* on page 25. For information about the Password Strength Enforced field, see *Password Strength Enforced* on page 397.

# Managing Notes

Depending on your permissions, you can manage notes on certain lists of objects or individual objects, such as doors, panels, and identities.

The **Notes** button displays the current number of notes for the list or object. If the notes belong to a list of objects, these notes relate to the list itself and are not partitioned.




Where available, click the **Notes** button to view, add, or delete notes.

# Initial Setup

After installing your ACM appliance, complete the following recommended setup procedures:

## Accepting the End User License Agreement

Before you can use the ACM system, you must accept the End User License Agreement.

1. In the top-right, select > **Appliance**.
2. In the About tab, click **View End User License Agreement Terms and Conditions**.
3. Review the license agreement then select the checkbox.
4. Click **Submit**.

Now you can license and configure the ACM system.

## Upgrading Your License Format

The ACM 6 license format is different from previous versions. If you upgraded from ACM 5.12.2 to ACM 6.0.0 or later, you will need to upgrade your license format in order to add new licenses. Do not add any new ACM 6 licenses until you have upgraded your old licenses.

**Note:** If your system is licensed for more than the maximum number of readers, you will not be eligible for an upgrade license. You can continue using your existing system, or contact sales to add more features.

If you do not upgrade your license format, you can continue to use your existing features. However, you will not be able to license new features.

**Important:** If you use the replication and failover features of the ACM system and you choose to upgrade the license format you must upgrade the license format on both the primary and standby ACM appliances. Replication features, including failover, will not function if the license format is not the same on both appliances. Complete the following steps on both appliances.

1. In the top-right, select >**Appliance**.
2. In the About tab, click **Download Upgrade File**.
3. Email the `.bin` file to acm.license@avigilon.com. You will receive a response in 1-2 business days with an Activation ID for each feature you have. You can continue to use the ACM appliance during this time.
4. After you receive the Activation IDs, follow the procedure in *Adding a License* on page 357. You will only need to enter one of the Activation IDs to automatically license the system for all features your device is entitled to.

# Adding a License

When you first install an ACM 6 system, you will need to license the system to use its features. Add additional licenses to access new features as required.

If you do not already have a license, purchase one from Avigilon.

When adding your first license, you must complete the appliance information on the **Appliance: Edit** page. At a minimum, ACM requires an **Appliance Name** and a **Host Name** to add a license. For information on completing information about the appliance, see *Editing Appliance Settings* on page 326.

## Online Licensing

If you have Internet access, use online activation. Otherwise, see *Offline Licensing* below.

1. In the top-right, select > **Appliance**.
2. In the About tab, click **Add License**.
3. In the Add Licenses dialog, enter your Activation IDs.
   - Click **Add ID** to add additional Activation IDs.
   - Click **Remove Last ID** to clear the last Activation ID entered.
4. Click **Activate Licenses**.

## Offline Licensing

Offline licensing involves transferring files between a computer running the ACM system and a computer with Internet access.

**In the ACM system:**

1. In the top-right, select >**Appliance**.
2. In the About tab, click **Add License**.
3. In the Add Licenses dialog, select the **Manual** tab.
4. Enter your Activation IDs.
   - Click **Add ID** to add additional Activation IDs.
   - Click **Remove Last ID** to clear the last Activation ID entered.
5. Click **Save File...** and select where you want to save the `.key` file. You can rename the file as required.
6. Copy the `.key` file to a computer with Internet access.

**In a browser:**

1. Go to activate.avigilon.com.
2. Click **Choose File** and select the `.key` file.
3. Click **Upload**.

> **Important:** When reactivating a site cluster, upload all the deactivation `.key` files first and then the single activation `.key` file at last.

A `capabilityResponse.bin` file should download automatically. If not, allow the download to occur when you are prompted.

4. Complete the product registration page to receive product updates from Avigilon.
5. Copy the `.bin` file to a computer running the ACC Client software.

**In the ACM system:**

1. In the Add Licenses dialog, click **Choose File**.
2. Select the `.bin` file and click **Open**.
3. Click **Activate Licenses**.

# Changing the Administrator Password

After you log in to the ACM application, you can change the `admin` identity's password.

1. Click **Identities** and then **Search**.
2. On the Identities list, click **A**.
3. Select the **Administrator, System** identity.
4. In the Account Information area, enter a new password in the **Password** and **Confirm** fields.
5. Click .

If you are currently logged in with the `admin` identity, you are automatically logged out. Log in again using the new password, or use a different Super Admin identity.

# Creating a Super Admin Identity

After you log in to the ACM system for the first time and set a new password, it is recommended that you create a Super Admin identity for configuring the system. By creating a new Super Admin identity, you can better protect the security of the system by not using the default `admin` identity, and having a backup identity in case the default `admin` password is lost.

1. Click **Identities** and then **Add Identity**.
2. Select an **Identity Profile** in the Identity Profile dialog box and click **Continue**.
3. In the Identity Information area, enter a **Last Name** and **First Name**.
4. In the Account Information area, enter a **Login** name for accessing the system.
5. In the **Password** and **Confirm** fields, enter a password for the new identity. The password must be at least four characters long.
6. Click and the Roles tab is automatically displayed.
7. In the Roles tab, select **Super Admin** from the Available list and click to assign the new identity to the Super Admin role.
8. Click .

Only these settings are required to create a Super Admin identity. You can add and configure more details for the account.

# Monitoring

The Monitoring screen gives you access to view all events and alarms in the system. It also allows you to view and control connected hardware. An event occurs for changes in the software or hardware. For example, when a user accesses a door. An alarm occurs when the system detects an unusual event. For example, a forced door. Hardware can be controlled to grant or restrict access to an area. For example, a door can be disabled to deny access to a hazardous area.

**Note:** If you do not have the correct delegations, you may not be able to access some of the following pages. See your System Administrator for details.

## Monitoring Events

Events are defined as any activity that is reported between the ACM appliance and the hardware it oversees. An event includes all alarms, but not all events are alarms. Events can include changes in configuration, a report on door access, adding a new badge holder to the system, and more. In other words, any transfer of data within the system is an event.

To view the events:

1. Select **Monitor** > **Events**.
2. Click any of the following buttons:

**Note:** Some of the buttons are disabled until you select an event that includes the relevant details.

- **Pause** button — Pauses the flow of events that are displayed on the page.

  The flow of events does not actually stop, the system simply pauses the display of live updates until you click **Resume**.
- **Resume** button — Restarts the flow of events that are displayed on the page.

  This button only appears when the flow of events is paused.
- **Clear** button — Temporarily clear all events from the screen. New events automatically begin to populate the list. To restore the cleared events, refresh the page.
- **Live Video** button — Displays live video that is associated with the selected event.
- **Recorded Video** button — Displays recorded video that is associated with the selected event.
- **Notes** button — Enter a new note or displays any previously saved notes for the selected event.
- **Instructions** button — Displays any instructions that should be completed when the event occurs. The instructions were added when the event was created.
- **Identity** button — Displays details about the person that triggered the selected event.
- **History** button — Displays a detailed history of this event.
- **Save Settings** button — Saves your current settings for this page. For example, the columns and order for this page.

- **Select Columns** button — Choose the information that you want displayed.

  Check the box for each column that you want to see, and clear the box for each column that you want hidden.

  Click and drag the columns to move them into the order you want.
- **Reconnect** button — Reconnects to the appliance.

  This button only appears if your browser has become disconnected from the appliance and an error is displayed.

## Pause/Resume Events

The display of live event updates can be paused. This allows you to view and investigate a specific event without having to search for it. Once the event has been reviewed, the display of live event updates can be resumed.

Follow the steps below to pause and resume events.

1. Click **Monitor** to access the Monitor Events page. For more detail see *Monitoring Events* on the previous page.
2. Click **Pause** to pause the flow of events that are displayed on the page.

   The flow of events does not actually stop, the system simply pauses the display of live updates until you click **Resume** (this button only appears when the flow of events is paused).
3. Click **Resume** to restart the flow of events that are displayed on the page.

   The list of events will resume updating.

## Clear Events

Follow the steps below to clear all displayed events.

1. Click **Monitor** to access the Monitor Events page.
2. Click **Clear** to temporarily clear all events from the screen.

   The list will be cleared. New events automatically begin to populate the list.

   **Note:** This does not delete the events, it just removes the existing events from the view. To restore the cleared events, refresh the page.

## View Live Video

Live video that is associated with a selected event can be displayed from the Monitoring Events page. For example, if an unusual event occurs, the live video can be viewed to observe the event and determine if any actions need to be taken.

Follow the steps below to view live video.

1. Click **Monitor**. The Monitor Events page displays (for more information, see *Monitoring Events* on the previous page).
2. Select an event from the list.

   Only events or alarms with an icon will have video.

3. Click **Live Video** to display live video that is associated with the selected event. (This button only displays if video is available for this event.)

   The Monitor Screen - Live Video window displays. View the live video in this window.

   If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## View Recorded Video

Recorded video that is associated with a selected event can be displayed from the Monitoring Events page. For example, if an unusual event occurred the previous day, the recorded video can be viewed to observe event and determine if any actions need to be taken.

Follow the steps below to view live video.

1. Click **Monitor**. The Monitor Events page displays (for more information, see *Monitoring Events* on page 26).
2. Select an event from the list.

   Only events or alarms with an icon will have video.
3. Click **Recorded Video** to display recorded video that is associated with the selected event. (This button only displays if video is available for this event.)

   The Monitor Screen - Recorded Video window displays. View the video in this window.

   If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## Create Event Notes

Notes can be added and viewed for all events that occur in the system. For example, if an observation is made on an event, a note can be made for that event.

Follow the steps below to create event notes.

1. Click **Monitor** to access the Monitor Events page.
2. Select the event that you want to create notes for.
3. Click **Notes** to create notes for the selected event.

   The Monitor Screen - Notes Window will display.
4. Enter text in the **New Note** field.
5. Click to save the new note.

   The note will display in the list below the **New Note** section. The date, Operator and note will display in this list.
6. Close the dialog box.

## View Event Notes

Notes that are associated with an event can be displayed from the Monitor Events page. For example, if another user created a note for an event, you can view the note to get more information about the event.

Follow the steps below to view event notes.

1. Click **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 26).
2. Select the event that you want to view notes for. (Events with notes will display with in the **Icon** column.)
3. Click **Notes** to view notes for the selected event. (Alternatively clicking will do the same thing.)

   The Monitor Screen - Notes Window will display. Existing notes will display as a list below the **New Note** section. The date, Operator and note will display in this list.

## View Event Instructions

Instructions can be viewed for a selected event. The instructions tell the operator what actions need to be taken when the event occurs. For example, if a user is denied access to a certain area, the action may be to review their identity, and determine if they have permission to access the area.

Follow the steps below to view event instructions. The instructions were added when the event was created.

1. Click **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 26).
2. Select the event that you want to view instructions for. (Events with instructions will display with in the **Icon** column.)
3. Click **Instructions** to view instructions for the selected event.

   The Monitor Screen - Instructions Window will display. View the instructions in the table that displays.
4. Close the window to return to the Monitor Events page.

## View Event Identity Details

Follow the steps below to view event identity details.

1. Click **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 26).
2. Select the event that you want to view identity details for.
3. Click **Identity** to view identity details for the selected event.

   The Monitor Screen - Identity Window will display.
4. View the details (e.g. Last Name, First Name, Title, etc.).
5. Close the window to return to the Monitor Events page.

## View Event History

Follow the steps below to view event history.

1. Click **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 26).
2. Select the event that you want to view history for.
3. Click **History** to view history for the selected event.

   The Monitor Screen - History Window will display.
4. View the history details.
5. Close the window to return to the Events list.

## Change Events List Settings

Follow the steps below to change the settings of the events list.

1. Click **Monitor** to access the Monitor Events page.

   The list displays in date order, with the most recent events at the top of the list.
2. If you want to re-sort the order of the list:
   - Click in the heading of the column to sort by (e.g. Priority). The list will sort in ascending order based on that column (e.g. ascending order of priority).
   - To change the sort order to descending, click the column heading again.
3. If you want to re-sort the order of the columns, click on the column you want to move then drag and drop this to it's new location.
4. If you want to add or remove columns, click **Select Columns** and:
   - Click beside the Column name of any columns to be added so that a check mark displays.
   - Click beside the Column name of any column to be deleted so that a check mark no longer displays.
5. Click **Save Settings** if you want to save the new settings.

   A message box displays with the message ACM Notification. Successfully saved.'.

## Reconnect to Events List

Follow the steps below to reconnect to the ACM appliance.

1. Click **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 26).

   If your browser loses connectivity with ACM appliance the **Reconnect** button displays.
2. Click **Reconnect** to reconnect.

# Searching for Events and Alarms

The number of alarms and event transactions can total into the thousands depending on the level of activity in your system. To find specific events, you can perform a search.

Searching for specific events allows you to easily find an event in the system. For example, searching for events can be used in situations where more information is needed on an event thought to be unusual or suspicious. Once an event has been found, information such as recorded video, or notes can be viewed.

1. Select **Monitor** > **Search**.
2. Scroll to the bottom of the page and click the icon.

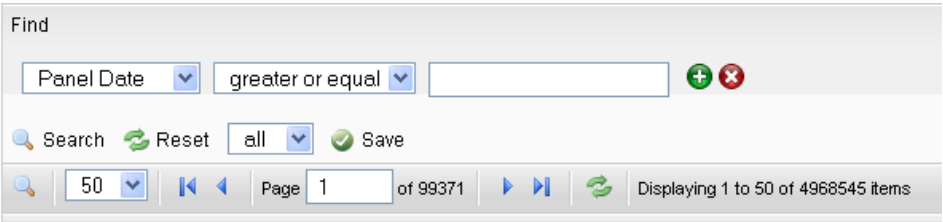
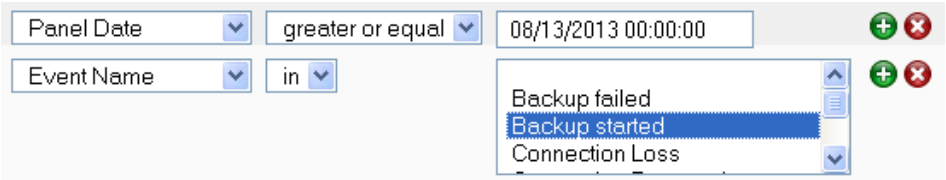



**Figure 1:** Search options

3. From the first drop down list, select the data type that you want to search. The options are:
    - Panel Date
    - Last Name
    - Card Number
    - Message
    - Event Name
    - Event Type
    - Source
4. From the second drop down list, select the appropriate argument for your search. The available arguments change depending on the selected data type. An argument may require you to make a selection, specify a date, or enter some text.

6. If you want to narrow your search further, click to add another search filter.

7. If you want to narrow your search, click to add another search filter.




8. Add as many search filters as you need to fulfill your search criteria.
9. When you have entered all your search criteria, click **Search**. The search results are listed in the table above the search area.
10. Select any transaction from the search result and use the action buttons at the top of the page to see the details of the event.

## View Camera (Search)

Live video that is associated with a selected event can be displayed from the Monitoring Search page. For example, if an event is found with live video associated with it, the operator can view the video and determine if any action needs to be taken.

Follow the steps below to view live video from a camera from the Events Search (Transactions) page.

1. Click **Monitor** > **Search**.
2. Select an event from the list.

   Only events or alarms with an icon will have video. The icons are not displayed by default. For more information, see *Change Transactions List Settings* on page 33.
3. Click **Camera** to display live video that is associated with the selected event.
4. View the live video in this window.

   If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## View Recorded Video (Search)

Recorded video that is associated with a searched event can be displayed from the Monitoring Search page.

For example, if an unusual event is found in the search results, the recorded video can be viewed to observe the event and determine if any actions need to be taken.

Follow the steps below to view live video from the Events Search (Transactions) page.

1. Click **Monitor** > **Search**.
2. Select an event from the list.

   Only events or alarms with an icon will have video. The icons are not displayed by default. For more information, see *Change Transactions List Settings* on the next page.
3. Click **Recorded Video** to display recorded video that is associated with the selected event.

   > **Note:** An event with recorded video associated with it may display an error message if the recorded video is no longer available on the video recorder.
4. View the video in this window.

   If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## Create Event Notes (Search)

Notes can be added and viewed for all events that occur in the system. For example, if an observation is made on an event, a note can be created for that event.

Follow the steps below to create event notes from the Events Search (Transactions) page.

1. Click **Monitor** > **Search**.
2. Select the event that you want to create notes for.
3. Click **Notes** to create notes for the selected event.

   The Monitor Screen - Notes Window will display.
4. Enter text in the **New Note** field.
5. Click to save the new note.

   The note will display in the list below the **New Note** section. The date, Operator and note will display in this list.
6. Close the dialog box.

## View Event Notes (Search)

Notes that are associated with an event can be displayed from the Monitor Search page. For example, if an event is found with an associated note, you can view the note to get more information about the selected event.

Follow the steps below to view event notes from the Events Search (Transactions) page.

1. Click **Monitor** > **Search**.
2. Select the event that you want to view notes for.
3. Click **Notes** to view notes for the selected event.

   The Monitor Screen - Notes Window will display. Existing notes will display as a list below the **New**

**Note** section. The date, Operator and note will display in this list.

## View Event Instructions (Search)

Instructions can be viewed for a selected event. The instructions tell the operator what actions need to be taken when the event occurs. For example, if a user is denied access to a certain area, the action may be to review their identity, and determine if they have permission to access the area.

Follow the steps below to view event instructions from the Events Search (Transactions) page. The instructions were added when the event was created.

1. Click **Monitor** > **Search**.
2. Select the event that you want to view instructions for.
3. Click **Instructions** to view instructions for the selected event.
   The Monitor Screen - Instructions Window will display.
4. Close the window to return to the Events Search (Transactions) page.

## View Event Identity Details (Search)

Follow the steps below to view event identity details from the Events Search (Transactions) page.

1. Click **Monitor** > **Search**.
2. Select the event that you want to view identity details for.
3. Click **Identity** to view identity details for the selected event.
   The Monitor Screen - Identity Window will display.
4. View the details (e.g. Last Name, First Name, Title, etc.).
5. Close the window to return to the Events Search (Transactions) page.

## View Event History (Search)

Follow the steps below to view event history from the Events Search (Transactions) page.

1. Click **Monitor** > **Search**.
2. Select the event that you want to view history for.
3. Click **History** to view history for the selected event.
   The Monitor Screen - History Window will display.
4. View the history details.
5. Close the window to return to the Events Search (Transactions) page.

## Change Transactions List Settings

The events list shows a default set of fields for each event. You may want to add columns to this list.

For example, if you want to search this list to see if an event occurred on a door that has a camera associated with it, add the icons column. This column displays a next to any event from a door that has a camera associated with it.

Follow the steps below to change the settings of the events list.

1. Click **Monitor** > **Search**.

   The list displays in date order, with the most recent events at the top of the list.
2. If you want to re-sort the order of the list:
   - Click in the heading of the column to sort by (e.g. Priority). The list will sort in ascending order based on that column (e.g. ascending order of priority).
   - To change the sort order to descending, click the column heading again.
3. If you want to re-sort the order of the columns, click on the column you want to move then drag and drop this to it's new location.
4. If you want to add a column, hover the mouse over any column heading and:
   a. Click the down arrow that is displayed.
   b. Click the checkbox for each column you want to add.
5. Click **Save Settings** if you want to save the new settings.

   A message box displays with the message 'ACM Notification. Successfully saved.'.

# Monitoring Alarms

Alarms that occur in the system are listed in the Monitor Alarms page as they occur (accessed through selecting **Monitor** > **Alarms**).

An alarm occurs when the system senses an unusual event such as a forced or held door. Each alarm needs to be reviewed and responded to. Information on the alarm can be viewed, along with any available video. After an alarm has been acknowledged, it is moved to the list of acknowledged alarms. This list allows users to view past alarms and clear them from the system.

To review and acknowledge alarms, select one or more alarms from the Unacknowledged Alarms list then click one of the following buttons:

**Note:** Some of the buttons are disabled until you select an event that includes the relevant details.

- **Acknowledge** — Click this button to acknowledge one or more selected alarms. The selected alarms are moved to the Acknowledged Alarms list.
- **Acknowledge All** — Click this button to acknowledge all alarms that are currently active and unacknowledged.
- **Live Video** — Click this button to display live video associated with the selected alarm.
- **Recorded Video** — Click this button to display recorded video associated with the selected alarm.
- **Notes** — Click this button to enter a new note or display any previously saved notes for the selected event.
- **Instructions** — Click this button to display any instructions that should be completed when the alarm occurs. The instructions were added when the event was created.
- **Identity** — Click this button to display details about the person that triggered the selected alarm.
- **History** — Click this button to display a detailed history of this alarm.
- **Assign** — Click this button to assign one or more selected alarms to a specific operator.
- **Save Settings** — Click this button to save your current settings for this page. For example, the columns and order for this page.

- **Sound Off** — Click this button to mute any alarm sounds on the device used to monitor Alarms.

  When sound is muted, the button changes to **Sound On**. Click this button to turn the sound back on.
- **Select Columns** — Click this button then choose the information that you want displayed.

  Check the box for each column that you want to see, and clear the box for each column that you want hidden.

After an alarm has been acknowledged, the alarm is added to the Acknowledged Alarms list. You can clear the alarms from the list as needed.

> **Note:** Some of the buttons are disabled until you select an event that includes the relevant details.

- **Clear** — Click this button to clear one or more acknowledged alarms from the list.
- **Clear All** — Click this button to clear all alarms from the Acknowledged Alarms list.
- **Select Columns** — Click this button then choose the information that you want displayed.

  Check the box for each column that you want to see, and clear the box for each column that you want hidden.

## Acknowledge Alarms

When an alarm occurs in the system, an action must be taken. Once the alarm is resolved, it must be acknowledged. This tells the other users of the system that the alarm has been dealt with and is not a problem.

Follow the steps below to acknowledge alarms.

1. Click **Monitor** > **Alarms**.
2. To acknowledge a single alarm:
   - Select the alarm in the Unacknowledged Alarms list.
   - Click **Acknowledge**. The alarm will move to the **Acknowledged Alarms** list.
3. To acknowledge multiple alarms:
   - Select the first alarm in the Unacknowledged Alarms list.
   - If the alarms to be acknowledged are consecutive in the list, click on the first entry, then hold SHIFT down and click on the last entry.
   - If the alarms to be acknowledged are not consecutive, click on the first entry, then hold CTRL down and click on each entry.
   - Click **Acknowledge**. The alarms will move to the **Acknowledged Alarms** list.
4. To acknowledge all alarms, click **Acknowledge All**. The alarms will move to the **Acknowledged Alarms** list.

## Assign Alarms

You can assign an alarm to an operator. After the alarm is assigned, you can see details about the alarm and its assignment.

You can add the Assignee column to the current display using the Select columns drop-down on the **Monitor** > **Alarms** page.

To assign one or more alarms:

1. Click **Monitor** > **Alarms**. The Monitor Alarms page displays (for more information see *Monitoring Alarms* on page 34).
2. Click on one or more alarms.

   To select a series of alarms, click the first alarm then **Shift** + click the last alarm in the series. To select non-contiguous alarms, **Ctrl** + click the alarms you want to select.
3. Click **Assign**.
4. Select an operator from the drop-down list.
5. Click **Save**.

   You can see the list of alarm assignments. You can also change or remove the assignee as needed.

## View Live Video (Alarms)

Live video that is associated with a selected alarm can be displayed from the Monitoring Alarms page. For example, if an alarm occurs, the live video can be viewed to observe the alarm and determine if any actions need to be taken.

Follow the steps below to view live video from the Monitor Alarms page.

1. Click **Monitor** > **Alarms**. For more information see *Monitoring Alarms* on page 34.
2. Select an alarm from the list.

   Only events or alarms with an icon will have video.
3. Click **Live Video** to display live video that is associated with the selected alarm. This button only displays if video is available for this alarm.

   The Monitor Screen - Live Video window displays. View the live video in this window.

   If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## View Recorded Video (Alarms)

Recorded video that is associated with a selected alarm can be displayed from the Monitoring Alarms page. For example, if an alarm occurred the previous day, recorded video can be viewed to observe the alarm and determine if any further actions need to be taken.

Follow the steps below to view recorded video from the Monitor Alarms list.

1. Click **Monitor** > **Alarms**. The Monitor Alarms page displays (for more information see *Monitoring Alarms* on page 34).
2. Select an event from the list.

   Only events or alarms with an icon will have video.
3. Click **Recorded Video** to display live video that is associated with the selected event. (This button only displays if video is available for this event.)

   The Monitor Screen - Recorded Video window displays. View the video in this window.

   If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## Create Event Notes (Alarms)

Notes can be added and viewed for all alarms that occur in the system. For example, if an observation or

action is made on an alarm, a note can be created to document the details.

Follow the steps below to create event notes from the Monitor Alarms page.

1. Click **Monitor** > **Alarms**. The Monitor Alarms page displays. For more information see *Monitoring Alarms* on page 34.
2. Select the event that you want to create notes for.
3. Click **Notes** to create notes for the selected event.

   The Monitor Screen - Notes Window will display.
4. Enter text in the **New Note** field.
5. Click to save the new note.

   The note will display in the list below the **New Note** section. The date, Operator and note will display in this list.
6. Close the dialog box.

## View Event Notes (Alarms)

Notes that are associated with an alarm can be displayed from the Monitor Alarms page. For example, if another user created a note for an alarm, you can view the note to get more information about the alarm.

Follow the steps below to view event notes from the Monitor Alarms page.

1. Click **Monitor** > **Alarms**. The Monitor Alarms page displays. For more information see *Monitoring Alarms* on page 34.
2. Select the event that you want to view notes for. Events with notes will display with in the **Icon** column.
3. Click **Notes** to view notes for the selected event. Alternatively clicking will do the same thing.

   The Monitor Screen - Notes Window will display. Existing notes will display as a list below the **New Note** section. The date, Operator and note will display in this list.
4. Close the dialog box to return to the Monitor Alarms page.

## View Event Instructions (Alarms)

Instructions can be viewed for a selected alarm. The instructions tell the operator what actions need to be taken when the alarm occurs. For example, if an alarm occurred, the instruction could be to investigate the alarm and write a note describing the situation.

Follow the steps below to view event instructions from the Monitor Alarms page. The instructions were added when the event was created.

1. Click **Monitor** > **Alarms** to access the Monitor Alarms page displays. For more information see *Monitoring Alarms* on page 34.
2. Select the event that you want to view instructions for. (Events with instructions will display with in the **Icon** column.)
3. Click **Instructions** to view instructions for the selected event.

   The Monitor Screen - Instructions Window will display. View the instructions in the table that displays.
4. Close the window to return to the Monitor Alarms page.

## View Event Identity Details (Alarms)

Follow the steps below to view event identity details from the Monitor Alarms page.

1. Click **Monitor** > **Alarms**. The Monitor Alarms page displays. For more information see *Monitoring Alarms* on page 34.
2. Select the event that you want to view identity details for.
3. Click **Identity** to view identity details for the selected event.

   The Monitor Screen - Identity Window will display.
4. View the details (e.g. Last Name, First Name, Title, etc.).
5. Close the window to return to the Monitor Alarms page.

## View Event History (Alarms)

Follow the steps below to view event history from the Monitor Alarms page.

1. Click **Monitor** > **Alarms** to access the Monitor Alarms page. For more information see *Monitoring Alarms* on page 34.
2. Select the event that you want to view history for.
3. Click **History** to view history for the selected event.

   The Monitor Screen - History Window will display.
4. View the history details.
5. Close the window to return to the Monitor Alarms page.

## Change Alarms List Settings

Follow the steps below to change the settings of the alarms lists on the Monitor Alarms page.

1. Click **Monitor** > **Alarms** to access the Monitor Alarms page. For more information see *Monitoring Alarms* on page 34.

   The list displays in date order, with the most recent events at the top of the list.
2. If you want to re-sort the order of the list:
   - Click in the heading of the column to sort by (e.g. Priority). The list will sort in ascending order based on that column (e.g. ascending order of priority).
   - To change the sort order to descending, click the column heading again.
3. If you want to re-sort the order of the columns, click on the column you want to move then drag and drop this to it's new location.
4. If you want to add or remove columns, click **Select Columns** and do the following:
   - Click beside the Column name of any columns to be added so that a check mark displays.
   - Click beside the Column name of any column to be deleted so that a check mark no longer displays.
5. If you want to change the sound settings:
   - If the sound is on, click **Sound Off** to turn the sound off.
   - If the sound is off, click **Sound On** to turn the sound on.
6. Click **Save Settings** if you want to save the new settings.

   A message box displays with the message 'ACM Notification. Successfully saved.'

**Note:** To reset default settings, select > **Clear Custom Layouts**. This resets all customized lists to their default setting.

## Turning Sound On/Off

You will be notified of an alarm if you are not watching the Alarms page. This is a useful way for operators to keep track of incoming alarms. The alarm sound is defined by the event.

To turn the sound off:

- On the Alarms page, click the **Sound Off** button.

  The sound is muted and the **Sound On** button appears.

To turn the sound on:

- On the Alarms page, click the **Sound On** button.

  The sound is audible and the **Sound Off** button appears.

# Using the Verification page

When you click **Monitor** > **Verification**, the Verification page is displayed.

This page allows a qualified operator to review information, including photos, about card holders entering or exiting specific doors.

The page is divided into two halves - the top Doors section and the bottom Events section.

- At the top of the page are four door panes that allow you to select and monitor four doors at a time. After you select a door to a pane, you can monitor live event transactions as they occur at that door.
- Underneath the door panes is a list of live door transactions displayed like the Events page.

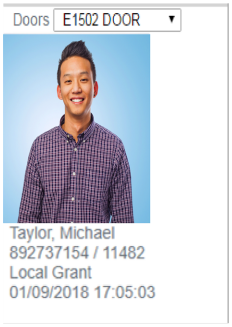
  Not all door events will display in this list. Only events in the priority number range 300 to 700 display. A full listing of all events is available on the Monitor Events page.

## Verifying Identities at Doors

Select **Monitor** > **Verification** to open the Verification page to verify and confirm the identity of any person who passes through the selected doors:

1. From one of the **Doors** drop down lists, select a door.
2. To select another door, repeat previous step in the other panes. The drop down list automatically updates to filter out the doors that have already been selected.

   When a person attempts to pass through one of the monitored doors using a card, the person's identity information is displayed:




If the person:

- Has a valid identity, the information includes the name and internal token number.
- Has a photo stored in the Identity record, it is displayed. If the person does not pass through the door, of the time and date of entry.
- Is authorized to pass through the door the time and date of entry is displayed, unless they do not actually pass through the door ("not used" is displayed instead).
- Is not authorized to pass through the door, an "Unauthorized" message is displayed.
- Presents an invalid identity, an "Invalid" message is displayed.

At the bottom of the screen are all of the detailed events generated at the doors, including those of any not associated with identities.

## Verification Events List

Follow the steps below to add doors to monitor on the Verification page.

1. Click **Monitor > Verification**. The Verification page displays. For more information see *Using the Verification page* on the previous page.

   This page has two sections - doors and an events list. For more information on the doors display see *Verifying Identities at Doors* on the previous page. The events list displays in date order, with the most recent events at the top of the list.

   > **Note:** Not all door events will display in this list. Only events in the priority number range 300 to 700 display. A full listing of all events is available on the Monitor Events page.

2. If you want to clear a single event from the list, select the event and click **Clear**. To clear all events, click **Clear all**.
3. If you want to re-sort the order of the list:
   - Click in the heading of the column to sort by (e.g. Priority). The list will sort in ascending order based on that column (e.g. ascending order of priority).
   - To change the sort order to descending, click the column heading again.
4. If you want to re-sort the order of the columns, click on the column you want to move then drag and drop this to it's new location.

5. If you want to add or remove columns, click **Select Columns** and:
    - Click beside the Column name of any columns to be added so that a check mark displays.
    - Click beside the Column name of any column to be deleted so that a check mark no longer displays.
6. Click **Save Settings** if you want to save the new settings.

   A message box displays with the message 'ACM Notification. Successfully saved.'.

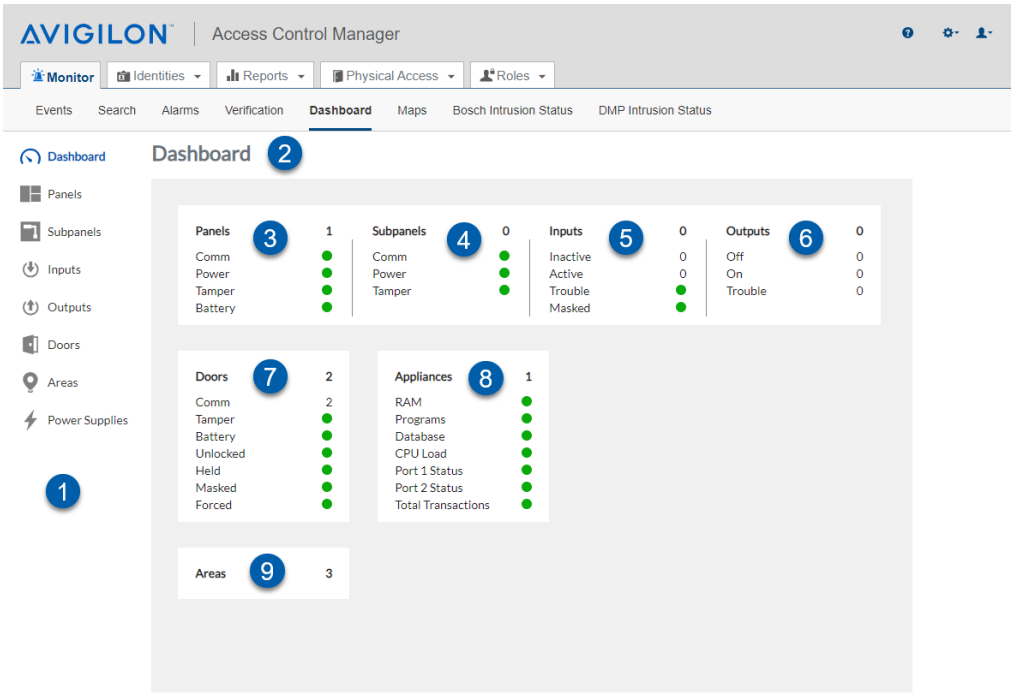
> **Note:** Saving the settings only saves the column configuration. The doors selected for verification will need to be selected each time you return to the page.

> **Note:** To reset default settings, select > **Clear Custom Layouts**. This resets all customized lists to their default setting.

# Using the Dashboard

The Dashboard provides a real-time status summary of the hardware components that are connected to the ACM system. The hardware categories are panels, subpanels, doors, inputs, outputs and ACM appliances.

Select **Monitor** > **Dashboard** for a top-level view of the Dashboard where you can drill down for details.



| | Area | Description |
|---|---|---|
| 1 | Dashboard Sidebar | Navigation menu for the Dashboard, Panels table, Subpanels table, Inputs table, Outputs table, Doors table, Areas table, and Power Supplies table ( if a LifeSafety power supply is connected).<br><br>From the Panels table, you can access a list of subpanels in the Subpanels table. From the Subpanels table, you can access a list of inputs and outputs in the Inputs and Outputs tables.<br><br>From the Inputs and Outputs tables, you can directly access the list of inputs and outputs.<br><br>From the Doors table, you can control individual doors, investigate doors with active faults, and see more information about the state of individual doors.<br><br>From the Areas table, you can view the details, including current identities, for each area. |
| 2 | Dashboard | Displays a summary of hardware faults or unexpected input and output state changes as they occur. As the status of hardware components changes, the status indicators on the Dashboard change color. For more information, see *Status Colors* on the next page.<br><br>The total number of connected hardware components (installed and uninstalled) is displayed above a real-time fault or status list. For panels, subpanels, inputs and doors, the number of installed components in each fault state is displayed. If no faults occur, their status is green. For outputs, the numbers indicate the number of installed outputs in each state. When no components are displayed in a state, the status is either green or 0. |
| 3 | Panels | Displays a summary of the fault state of the installed panels. Click the number next to the fault to drill down to the details of the fault in the Panels table, which is filtered to display only the panels with that fault. |
| 4 | Subpanels | Displays a summary of the fault state of the installed subpanels. Click the number next to the fault to drill down to the details of the fault in the Subpanels table, which is filtered to display only subpanels with that fault. |
| 5 | Inputs | Displays the total number of inputs in each state. Click the number next to the state to drill down to the Inputs table, which is filtered to display only inputs with that state. |
| 6 | Outputs | Displays the total number outputs in each state. Click the number next to the state to drill down to the Outputs table, which is filtered to display only inputs with that state. |
| 7 | Doors | Displays the summary of the fault state of the installed doors. Click the number next to the fault to drill down to the Doors table, which is filtered to display only alarms with that fault. |
| 8 | Appliances | When no issues occur in the ACM appliance items, their status is green. Hover the mouse over each status indicator to see more details. For example, "RAM free 45%" displays for the RAM status. |
| 9 | Areas | Indicates the number of defined areas. |

## Status Colors

Status colors identify the health of the different devices in the system. The status colors represent the following states:

| Color | Status | Description |
|---|---|---|
| | Normal | Online and working properly. |
| | Inactive | Input or output is in its normal state. |
| | Trouble | Indeterminate or offline status of inputs, outputs, panels or subpanels, and the ACM appliance. Inputs or outputs may be operating in a wiring fault state. |
| | Alarm | Alarm condition. An ACM operator should investigate the problem and resolve the issue. |
| | Active | Input or output circuit is no longer in its normal state. |
| | Masked | Input is currently masked. Its actual state is not displayed. Masked inputs are intended to change as part of normal operations, so that they are not constantly being reported. |

## Appliance Transactions Indicators

The status colors represent the following appliance states:

| Color | Status | Description |
|---|---|---|
| | Normal | The appliance transactions stored in the system are less than 85% of the maximum stored transactions threshold. |
| | Trouble | The appliance transactions stored in the system are between 85% - 95% of the maximum stored transactions threshold. |
| | Alarm | The appliance transactions stored in the system are over 95% of the maximum stored transactions threshold. |

**Tip:** When the transactions are close to exceeding the maximum stored transactions threshold, do the following:

- Schedule backups of the transactions before their deletion.
- Increase the Max Stored Transactions setting.
- Adjust the Max Days Stored setting, according to your corporate IT policy.

## Device Status

Panels, Subpanels, Inputs, Outputs and Doors only.

To see the legend for device status:

- Click **Legend** to see the list of statuses and the related icons. For other input statuses which appear in the legend, see *Status Colors* above.

**Note:** Not all statuses apply to devices. For example, only normal, uninstalled, communication and battery statuses apply to Control locks.

| Icon | Status | Description |
|---|---|---|
| | Normal | The panel, subpanel or door is operating normally. |
| | Uninstalled | The panel, subpanel, input, output or door is not installed. |
| | Communication | Communication between the panel, subpanel or door, and the ACM system is enabled. |
| | Unlocked | The door is unlocked and is not secure. |
| | Held | The door is being held open. |
| | Power | The panel or subpanel power input circuit is open. |
| | Battery | The battery input circuit is open or is running low. |
| | Tamper | The tamper input circuit is open. |
| | Forced | The door was forced open without a grant operation. |
| | Synchronization | Synchronization between the door and the ACM system is pending. |
| | Synchronization | Synchronization between the door and the ACM system is out of sync.<br><br>*ASSA ABLOY IP door.* The out of sync door requires operator intervention to reload or reset the lock. For more information, refer to ASSA ABLOY documentation.<br><br>*SALTO online door.* Wait for the update.<br><br>*SALTO standalone door.* Requires operator intervention. Use the portal programming device (PPD) to update the door mode. For more information, refer to SALTO systems documentation. |

## Security Status

To see the legend for device status:

- Click **Legend** to see the list of statuses and the related icons.

| Icon | Status | Description |
|---|---|---|
| | TLS Required | The panel is configured to use Transport Layer Security (TLS) protocol to secure communication with the ACM appliance. |
| | TLS & Certificate Required | The panel is configured to use TLS protocol and a certificate to secure communication with the ACM appliance. |

## Installing, Uninstalling and Deleting Panels and Subpanels

Click ··· at the end of a row in the Panels table or Subpanels table to:

- **View** — Displays the Panel: Status or Subpanel: Status table.
- **Install** — Enables communications between the ACM system and the panel or subpanel.
- **Uninstall** — Disables communications between the ACM system and the panel or subpanel.
- **Delete** — Removes the connection between the ACM system and the panel or subpanel.

## Viewing, Masking and Unmasking Inputs

Panels, Subpanels and Inputs only.

- Click ··· at the end of a row in the Inputs table to:
  - **View** — Displays the Input: Edit page.
  - **Mask** — Masks the selected input.
  - **Unmask** — Unmasks a previously masked input.

## Viewing, Activating and Deactivating Outputs

Panels, Subpanels and Outputs only.

1. Click the name of the panel and subpanel to display the Outputs table.

   Or click **Outputs** on the Dashboard home page.

2. Click ··· at the end of a row in the Outputs table to:
   - **View** — View the Output: Edit page.
   - **On** — Power the output. If the output is a door, it activates the circuit.
   - **Off** — Turn off the power to the output. If the output is a door, it deactivates the circuit.
   - **Pulse** — Alternately activate and deactivate the output. The pulse interval is determined by the output's settings.

## Searching Panel, Subpanel, Input and Door Names

Panels, Subpanels, Inputs and Doors only.

1. Use any (or all) of the following to define your search:
   - Enter your search term in the **Search...** field. Use any series of letters and numbers to search for the panels you want to see.

- If known, select the **Device Status**.
- If known, select the **Appliance** the panel is connected to.
- If known, select the **Group** the panel is included in.

2. Click **OK**. The list is filtered to show the results of your search.

## Saving Door Filters

Many facilities require the control and monitoring of dozens, even hundreds, of doors simultaneously. This can result in a crowded listing page. You can search for specific doors to narrow the list of doors, filter the columns for specific values, and create and save custom filters. You can then sort the results using any one column.

1. Click **Advanced Filters** in the upper-right corner.
2. Select filters:
   - **Alarms** — Includes the alarms from the list of alarms.
   - **Masked** — Includes the masks from the list of masks.
   - **Normal** — Includes all properly functioning doors.
   - **Door Mode** — Includes the list of door modes.

   To unselect all selected filters, click **Unselect All**.
3. To save the selected filters, select **Remember Filters**.
4. Click **OK**.

## Controlling Doors

While you are monitoring the system, you may need to override the default door settings to allow a visitor access to an area, or unlock a door in an emergency situation. From a Doors listing page in **Physical Access** or **Monitor > Dashboard**, use the Door Action, Door Mode, Forced, Held, and Installed drop-down menus to control doors.

Doors can also be controlled from **Monitor > Maps**. For more information, see *Using a Map* on page 432.

> **Note:** Only the Installed options are available for virtual doors installed for use with ACM Verify readers.

1. Select the checkbox for each the door you want to control.

   Or click **All** at the top of the left column to select all doors or **None** to deselect all doors.
2. For one or more doors, select a **Door Action** if required:

   > **Note:** The door actions below are not applicable for Schlage offline Wi-Fi doors or SALTO standalone doors. Only Grant is applicable for Schlage Control™ locks. Only Unlock and Locked No Access are applicable for Von Duprin remote undogging (RU) devices. Locked No Access and Disable are not applicable for ASSA ABLOY battery-powered and external-powered doors.

- **Grant** — Momentarily grants access to the door to permit a single-time entry.
- **Restore** — Restores the Door Mode to its default configuration or Custom Mode.

  *Schlage locks with activated lock functions only.* Restoring a door that has an activated Lock Function (Classroom, Office, Privacy, or Apartment) removes the Lock Function and resets the door mode to its default configuration.

  *For ASSA ABLOY IP doors only.* Restoring a door results in the door going offline temporarily in the ACM system.
- **Unlock** — Unlocks the door. The door remains unlocked until the **Locked No Access** command is issued or until an operator override or scheduled action is initiated.
- **Locked No Access** — Locks the door. The door remains locked until the **Restore** command is initiated or until an operator override or scheduled action is initiated.
- **Disable** — Disables the door. The door stops operating and allows no access to anyone.
- **Lock (ASSA ABLOY Only)** — *For ASSA ABLOY IP doors only.* Locks the door. The door remains locked until a scheduled action is initiated.

3. Select any of the following **Door Mode** options to change the door mode.

   For more information, see *Door Modes* on page 203.
4. Select either of the following **Forced** options if required:
   - **Mask Forced** — Masks the Forced Door Alarm for the door. The status color changes to blue and is no longer included in any alarm subtotal.
   - **Unmask Forced** — Unmasks the Forced Door Alarm for the door.
5. Select either of the following **Held** options if required:
   - **Mask Held** — Masks the Door Held Open Alarm for the door.
   - **Unmask Held** — Unmasks the Door Held Open Alarm for the door.
6. Select either of the following **Installed** options if required:
   - **Install** — Installs a door. Enables communication between the door and the ACM system.
   - **Uninstall** — Uninstalls a door. Disables communication between the door and the ACM system.
7. Select **Delete** — Removes the connection between the door and the ACM system.

## Accessing Web Interface of Power Panels

When LifeSafety power panels are installed in your ACM system, you can access the web interface of the panel to view the panel's current status or its event log, and edit its configuration.

- Click the name of the LifeSafety power panel to display the panel details.
- The (installed) or (uninstalled) status of the panel is read-only and cannot be changed.
- Click a command:
  - **Status** — Displays the current status of the LifeSafety panel.
  - **Log** — Displays the log of events and alarms recorded by the LifeSafety panel.
  - **Edit** — Displays the browser page for the remotely connected panel. Edit the configuration as required.

# Using Map Templates

Click **Monitor** > **Maps** to display all the maps that have been added to the system.

# Using a Map

Access a map of your site, facility or floor plan from the Monitor page to do any of the following:

- Monitor the status of doors, panels, subpanels, inputs and outputs that are installed. For example, a mustering station on the third floor of a building.
- Set the door mode and door commands on the map.

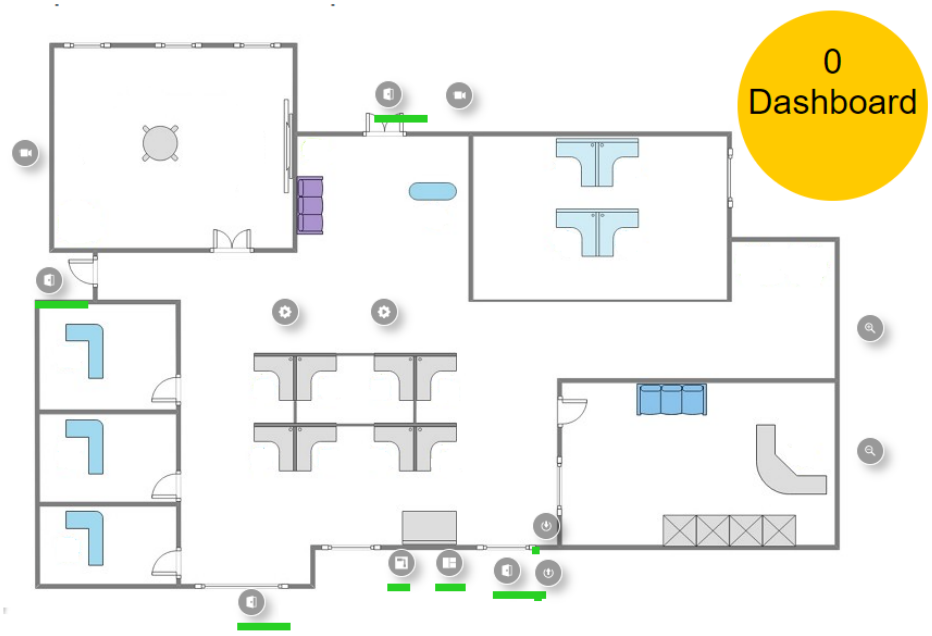
> **Note:** Unlike the Physical Access > Doors or Monitor > Dashboard page which displays all modes and commands regardless of door type, the Monitor > Maps page displays only the modes and commands that are supported by your door or device.

- Keep track of identities as they arrive at muster stations from the Mustering dashboard.

## Viewing a Map

To access and monitor your site from a map:

1. Select **Monitor > Maps**.
2. In the Map Templates list, click **Show** next to the name of a map.
   Some of the displayed elements may not appear in your map or the example below.




> **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| Field | Icon | Field | Icon |
|---|---|---|---|
| **Doors** | | **Cameras** | |
| **Panels** | | **Zoom In** | |
| **Supbpanels** | | **Zoom Out** | |
| **Inputs** | | **Global Actions** | |
| **Outputs** | | **Dashboard Elements** | Square, circle, or text object |

## Hardware Status

The following indicators are displayed on the map as events occur:

| Icon | Status | Description |
|---|---|---|
| | Green bar | The hardware is operating normally. |
| (13) | Red square | The hardware is in an alarm state. The counter in the square shows the number of unacknowledged events. |
| (6) | Solid blue disk | An active override is in effect on the door. |
| | Hollow blue disk | An inactive override is defined. |
| | Red bounding box around the status bar | The door is in Priority Mode. |

## Map Actions

The actions you can complete on a map are determined by the permissions of your assigned roles.

| To... | Do this... |
|---|---|
| Review hardware status | The colored bar below each item displays an overview of the current communication and power status.<br>• Click the icon on the map to display the control menu.<br>For more information about the colored hardware status bar, see the specific hardware status page. For more information about the status colors, see *Status Colors* on page 43. |

| To... | Do this... |
|---|---|
| Review an alarm | If you see a red alarm indicator, the item on the map is in an alarm state.<br>• Click the alarm indicator to see the status details.<br>For more information about alarm actions, see *Monitoring Alarms* on page 34. |
| Modify or delete an override | If you see solid blue disk indicator, an active override is in effect on the door. If you see a hollow blue disk indicator, an inactive override is defined.<br>• Click the indicator to open the Doors: Overrides page to see details. |
| Respond to a priority situation | If you see a red bounding box around the status indicator, the door is in Priority Mode.<br>**Important:** A door is in Priority Mode when a priority situation has been declared at your site. All doors affected by the situation are placed into Priority Mode and only the Priority ACM Operator, responsible for dealing with priority situations can interact with the door. |
| Control a door | Click on the map to display the control menu for the selected door.<br>**Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.<br>Use the menu options to set the Door Mode. For more information, see *Door Modes* on page 203.<br>Use the following menu options to mask or unmask alarms:<br>• **Mask Held** — Mask the Door Held Open Alarm.<br>• **Unmask Held** — Unmask the Door Held Open Alarm.<br>• **Mask Forced** — Mask the Door Forced Open Alarm.<br>• **Unmask Forced** — Unmask the Door Forced Open Alarm.<br>To view live video, recorded video, notes, instructions, identities, and history click **Trace** to display the event transactions for the door.<br>To hide the control menu, click the icon again. |

| To... | Do this... |
|---|---|
| Control a panel or subpanel | Click or on the map to display the panel control menu, and then for the panel or subpanel use these options:<br>• Panels<br>  ◦ **Download Params** — Download the latest system configurations to the panel.<br>  ◦ **Tokens** — Download the tokens to the panel.<br>  ◦ **Reset/Download** — Reset and download the current system configuration to the panel.<br>  ◦ **APB Reset** — Resets all panel and area counts to zero.<br>  ◦ **Clock** — Re-sync the panel time.<br>  ◦ **Trace** — Display the event transactions for the panel.<br>  **Note:** This is the only option supported for ASSA ABLOY IP panels.<br>• Subpanels<br>  ◦ **Trace** — Display the event transactions for the subpanel.<br>Viewing live video, recorded video, notes, instructions, identities, and history can be performed on the event transactions.<br>To hide the control menu, click the icon again. |
| Control an input | Click the on the map to display the input control menu for the input.<br>Use these options to mask or unmask the input:<br>• **Mask** — Mask the input.<br>• **Unmask** — Unmask the input.<br>To hide the control menu, click the icon again. |
| Control an output | Click the on the map to display the output control menu for the output.<br>Use these options to initiate output actions:<br>• **On** — Activate the output.<br>• **Off** — Deactivate the output.<br>• **Pulse** — Pulse the output.<br>To hide the control menu, click the icon again. |
| Display video | Click the on the map to display the Camera Video window. |
| Open a linked map | Click to display a linked map, or to display a linked map. |

| To... | Do this... |
|---|---|
| Monitor the dashboard | If there is a Mustering dashboard configured on the map, it may appear as a line of text or as a shape with text inside.<br>The dashboard displays the number of identities in the area and may include the name of the area. In *Using a Map* on page 48, the dashboard is the gray square.<br>Click the dashboard to see a list of all the identities that are in the area. Click outside the pop-up dialog to hide the identities list. Click the First Name or Last Name to view the identity. |

## Adding Maps

Follow the steps below to add maps.

1. Click **Monitor** > **Maps**. The Map Templates (Monitor) list displays.
2. Click **Add Map Template**.
3. Enter a name for the map in the **Name** field.
4. Do one of the following:
   - To upload the image file for the map, click **Choose File** and then click **Open**.
   - To not use a background, select **Blank Canvas**.
5. Click **Save**.

# Monitoring Bosch Intrusion Panels

The following procedures relate to monitoring Bosch intrusion panels.

## Monitor Bosch Intrusion Panel Status

The intrusion panel status displays the current status of all connected intrusion panels. For example, if the power and communications of the intrusion panel is normal, the Online status will be displayed and a message will appear when you hover over the power and communications icons.

To monitor intrusion panel status:

1. Select **Monitor** > **Bosch Intrusion Status**.
2. View the list that displays.

   The following statuses display for panels:
   - Communications
   - Battery
   - Power
   - Tamper
   - Phone Line

   The following statuses apply to all of the above:

   Online

   Alarm

Trouble

> **Note:** To view more detail on the status, hover over the status icon to view a pop-up message (e.g. hovering over an Alarm status indicator in the **Comm** column might return the message 'Not connected, verify configured IP and port').

3. If you want to narrow the list that displays use the filter function. Enter a panel name to filter the list results by panel. Type in the name (or part of the name) of the panel and the list will update as you type.
4. If you want to sort the list, click ▲ to sort in ascending order, or ▼ to sort in descending order in each column.

# Monitoring Areas in Bosch Intrusion Systems

> **Note:** If displays on the **Areas** tab, it indicates at least one of the areas is in alarm.

## Viewing Areas

To monitor the areas of all connected intrusion panels and send commands to them:

1. Select **Monitor** > **Bosch Intrusion Status**.
2. Click the **Areas** tab.

   A status is displayed for each area.

   Armed

   Ready to Arm

   Not Ready to Arm

   Partial Arm

   Trouble

   Alarm

   > **Note:** To view more detail on the status, hover your mouse over the status icon to view a tooltip. For example, hovering over an Armed status indicator displays 'All On Instant Arm'.

3. To find an area quickly, do any of the following:
   - Type the area name in the **Filter** box.
   - Select a status in **Status**.
   - Click the column heading to sort the lists.

### Arming Areas

1. Select the areas to be armed.
2. Click **Primary** and select the arming option.
    - **Instant Arm** - Arm all points for the selected areas instantly.
    - **Delay Arm** - Arm all points for the selected areas with an entry/exit delay.
    - **Force Instant Arm** - Arm all points for the selected areas instantly, regardless of their current state.
    - **Force Delay Arm** - Arm all points for the selected areas with an entry/exit delay, regardless of their current state.

### Arming Perimeter Areas

1. Select the areas to be armed.
2. Click **Perimeter** and select the arming option.
    - **Instant Arm**
    - **Delay Arm**
    - **Force Instant Arm**
    - **Force Delay Arm**

### Disarming Areas

1. Select the areas to be disarmed.
2. Click **Disarm**.

### Silencing Keypad Alarms

1. Select the areas that are in alarm.
2. Click **Silence**.

### Clearing Alarms

1. Select the areas that are in alarm.
2. Click **Clear Alarms**.

### Resetting Sensors

1. Select the areas.
2. Click **Reset Sensors**.

   The reset time is 5 seconds. During the reset time, alarms from the points associated with the selected areas will be ignored.

## Monitor Bosch Intrusion Panel Points

The intrusion panel points displays the current status of all connected points. For example, if a point has been bypassed, the bypassed status will display and a message will appear when you hover over the status icon.

To monitor intrusion panel point status:

1. Select **Monitor > Bosch Intrusion Status**.
2. Click the **Points** tab.
3. View the list that displays. A status is displayed for each point.

   The following statuses apply to all of the above:

   Normal

   Faulted

   Bypassed

   Trouble

   > **Note:** To view more detail on the status, hover over the status icon to view a pop-up message (e.g. hovering over an Bypassed status indicator might return the messages such as 'Open', 'Missing' or 'Normal').

4. If you want to narrow the list that displays, either:
   - Use the filter function. Enter a point name to filter the list results by point. Type in the name (or part of the name) of the point, area, or panel and the list will update as you type.
   - Select a single status (e.g. Faulted) to view.
5. If you want to sort the list, click to sort in ascending order, or to sort in descending order in each column.
6. If you want to bypass or unbypass a point:
   - Select the point (or points) in the list, and
   - Click either the **Bypass** or **Unbypass** button.

   > **Note:** Some points in the system may not be bypassed due to configuration settings. Trying to bypass these points will result in no state change.

## Monitor Bosch Intrusion Panel Outputs

The Bosch intrusion panel outputs display the current status of all connected outputs. For example, if a output is active, the Active status will display and a message will appear when you hover over the status icon.

To monitor intrusion panel outputs status:

1. Select **Monitor > Bosch Intrusion Status**.
2. Click the **Outputs** tab.
3. View the list that displays. A status is displayed for each output - the available statuses are:

   Inactive

   Active

   Trouble

4. If you want to narrow the list that displays, either:
    - Use the filter function. Enter an output name to filter the list results by output. Type in the name (or part of the name) of the output, or panel and the list will update as you type.
    - Select a single status (e.g. Active) to view.
5. If you want to sort the list, click to sort in ascending order, or to sort in descending order in each column.
6. If you want to activate or deactivate an output:
    - Select the outputs in the list, and
    - Click either the **Activate** or **Deactivate** button.

# Monitoring and Controlling DMP Intrusion Systems

Select **Monitor** > **DMP Intrusion Status** to monitor the status of all connected DMP intrusion panels, areas, zones and outputs, and send commands to them.

## Viewing Panels, Areas, Zones and Outputs

**Note:** is displayed when at least one of the objects in the tab is in Critical or Unknown condition.

- Type the name of the panel, area, zone or output in the filter box ( ) in their respective tabs.
- Click to enter a checkmark to filter items by the following statuses.

| | |
|---|---|
| **Normal** | Online and working.<br>Examples: Area is armed. Zone is in the expected state. |
| **Warning** | Warning condition.<br>Examples: Area is disarmed. Zone is bypassed. |
| **Critical** | Critical condition.<br>Examples: Area is armed with alarm. Zone is in not in the expected state or in alarm state. |
| **Unknown** | Unknown condition. |

- Panels tab only. View the connection status.

| | |
|---|---|
| **Encryption Fails** | Encrypted connection or remote key failed.<br>For more information about the panel setting, see *Panel Encryption* on page 426. |
| **Incompatible** | DMP firmware version is not supported.<br>For more information, see *Prerequisites* on page 425. |
| **Offline** | Panel is not connected. |
| **Online** | Panel is online. |

> **Tip:** Hover your mouse over the status box to view a tooltip.

- Click the column heading to sort the lists.

## Silencing Keypad Alarms on Panels

1. Click the **Panels** tab.
2. Select one or more panels.
   To select all items, click the first column heading.
3. Click **Silence Alarm**.

## Resetting Sensors on Panels

1. Click the **Panels** tab.
2. Select one or more panels.
   To select all items, click the first column heading.
3. Click **Reset Sensors**.

## Arming or Disarming Areas

1. Click the **Areas** tab.
2. To arm an area:
   a. Select one or more areas in **Disarmed** status.
      To select all items, click the first column heading.
   b. In **Bad Zone Action**, select the action for a zone in an area that might not be in the expected condition at the time of arming.
      - **Bypass**: All bad zones are bypassed.
      - **Force**: All bad zones are force armed.
      - **Refuse**: No zones are armed until the zone is restored.
   c. Click **Arm**.
      The area is Armed.
3. To disarm an area:
   a. Select one or more areas in **Armed** status.
      To select all items, click the first column heading.
   b. Click **Disarm**.
      The area is Disarmed.

## Bypassing Zones and Resetting Bypassed Zones

1. Click the **Zones** tab.
2. To bypass a zone:
   a. Select one or more zones in **Open** alarm status.
      To select all items, click the first column heading.
   b. Click **Bypass**.
3. To reset a bypassed zone, click **Reset Bypassed**.
   The zones in the area are Armed.

## Activating and Deactivating Outputs

1. Click the **Outputs** tab.
2. To activate an output:
   a. Select one or more outputs in **Off** (unpowered) status.
      To select all items, click the first column heading.
   b. In **Activate**, choose:
      - **Steady**: Turns on and remains 'on' until the area is disarmed, an output cutoff expires, or the output is reset.
      - **Momentary**: Turns on only once for one second.
      - **Pulse**: Alternates one second 'on' and one second 'off.'
      - **Temporal Code**: For the duration of the bell cutoff time, repeats half second 'on' and half second 'off' (three times) followed by 2.5 seconds 'off.'
   c. The output is On (powered).
3. To deactivate an output:

a. Select one or more outputs in **Pulse** (intermittently on and off) or **On** status. To select all items, click the first column heading.
b. Click **Deactivate**.
c. The output is Off (unpowered) status.

# Identities

The Identities screen gives you access to all tokens and operators of the system. An identity is added to the system when a new user needs access to the site. For example, when a person is hired. Access to a site may be physical access to an area or access to the ACM system to manage the site.

Physical access to the site allows a user to access areas and doors. Access to the ACM system allows users to manage the site, such as adding users or monitoring events.

For a user to have access to the system or physical access to the site, they must have an identity.

- If the user requires access to the system, they are issued a login and password. This allows the user to access areas of the system. The areas of the system the user has access to depends on their role.
- If a user requires physical access to the site, they are issued a token. The token gives the user physical access to the site. This allows the user to access areas on the site. The areas the user has access to depends on their role in the system.

**Note:** If you do not have the correct delegations, you may not be able to access some of the following pages. See your System Administrator for details.

## Setting Up Multi-Factor Authentication

For extra security, you can enable multi-factor authentication (MFA) and have your identity information be authenticated with the assistance of a third-party app when logging in to the ACM system. You enter your password first and then the code generated on your device for two-step identity verification.

**Tip:** Use a standard Time-based One-Time Password (TOTP) compatible app.

### Add Your MFA Devices

Add one or more MFA devices that can generate a temporary passcode for two-step identity authentication at time of login. You can add up to five devices.

Contact your ACM administrator for permission to manage MFA devices. For more information, see *Permissions and Rights for MFA* on page 487.

#### Add MFA Device

**Note:** Before you start, ensure a TOTP app is installed and configured on your desktop or mobile device.

1. Go to > **My Account**.
2. On the Profile tab, click **Add New Device** next to MFA Device.

   **Note:** Enabling the MFA for an identity will prevent the identity from using the ACM Expedite Mobile App, Avigilon Control Center (ACC) and ACM unification solution, and ACM REST API applications.

3. Enter your current password in **Password**.
4. Click **Next**. A QR code is generated.
5. Follow the instructions to set up the app and scan the QR code using your mobile device.

   If your mobile device cannot scan or you are using a desktop app, click **Can't scan?** to display the contents of the QR code. Go to your app and type the code.
6. In **Name your device**, enter a name and click **Next**.
7. Enter the six-digit code generated by the app and click **Verify**. The device is added.

Next, see *Logging In* on page 21.

**Note:** If your password is reset by the ACM administrator or another operator, all your MFA devices will be deleted.

### Delete MFA Device

1. Click next to MFA Device.
2. Click **OK**.

## Disable MFA

1. Go to **Identities** > **Identities**.
2. On the Identity tab, remove the checkmark in the **Multi-Factor Authentication** field.
3. Click **OK**.
4. Click **Save**. The field becomes read-only.

**Note:** Disabling the field will remove the user's MFA devices.

# Configuring HID Mobile Access® Credentials

Before you can issue HID Origo tokens, you must configure HID Origo. For more information, see:

- *Prerequisites* below
- *Step 1: Connecting to the HID Origo External System* below
- *Step 2: Enrolling Identities and Issuing Tokens* on the next page

## Prerequisites

You need access to HID Origo configuration information in the HID Origo Management Portal.

1. Create an HID Origo account, log in and go to **Organization Administration**.
2. Add a **System Account** and enable **Mobile Identities** to communicate with ACM.
3. Select the **Password** credential type and enter a password. (Only password credentials are supported by ACM. PKI credentials are not supported.)

For more information, refer to HID mobile access documentation.

## Step 1: Connecting to the HID Origo External System

**Note:** Before you begin, obtain the Organization ID and user account information from the HID Origo Management Portal.

**Important:** Connecting more than one ACM system to the same HID Origo account is not recommended.

To connect to HID Origo in ACM:

1. Select > **External Systems**.
2. Click the **HID Origo** tab.
3. Enter:

| | |
|---|---|
| **Appliance** | The name of the ACM appliance. |
| **Authentication Portal** | The URL of the HID authentication portal. |
| **Management Portal** | The URL of the HID management portal. |
| **Customer ID** | The Organization ID. |
| **User Name** | The Client ID of the system account. |
| **Password** | The password for the system account. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Installed** | Enables communication between the ACM appliance and HID Origo after saving. |

4. Click the **Create** button.

After the connection is saved, see *Step 2: Enrolling Identities and Issuing Tokens* below.

## Step 2: Enrolling Identities and Issuing Tokens

**Note:** Before you begin, configure the Enroll Settings section in the HID Origo Management Portal.

To enroll an identity and issue an HID Origo token:

1. Select **Identities** > **Identities** and click **Search** to select an identity already created.

   If you need to add an identity, see *Adding an Identity* on page 65.

   If you need to add a role, see *Adding an Access Group* on page 105 and *Assigning an Access Group to a Role* on page 107.
2. Click the **Tokens** tab and enter:

| | |
|---|---|
| **Token Type** | HID Origo |
| **Mobile ID Type** | The mobile ID to be issued to the registered device. |

   For other field descriptions, see *Token Fields* on page 76.
3. Click **Enroll**. An invitation is sent to the email address of the identity.
4. Instruct the identity to follow the steps in the email, including clicking an app store link to install the HID Mobile Access app and then clicking the invitation code link to enroll.
5. After the identity accepts the invitation, the HID Origo token will be available in their mobile app.

### Issuing a Token to an Enrolled Identity on a Registered Mobile Device

If you need to issue to an identity an additional credential with a different mobile ID, you can issue another token:

1. Click **Add Token** on the Tokens tab and enter:

| | |
|---|---|
| **Token Type** | HID Origo |
| **Mobile ID Type** | The HID mobile card that is not already issued to the device. |

2. Click **Issue Token**.
3. Select the mobile device in the Device Selector.
4. Click **Submit**. The token is displayed in the list of tokens in the ACM application. Another token is displayed in the HID Mobile Access app.

### Registering a New Mobile Device for an Enrolled Identity

If an identity has swapped devices or if an invitation has expired, you can send another invitation:

1. Click **Send Invitation** on the Tokens tab.
2. Instruct the identity to follow the steps in the email, including clicking an app store link to install the HID Mobile Access app and then clicking the invitation code link to enroll.

## Searching for HID Origo Tokens

To search for HID Origo tokens that were issued, or are being issued, to identities:

1. Select **Identities** > **Identities**.
2. Use **Identity Search** to find an identity.
   - In Search Field, select **HID Origo Token Status**.
   - In Search Value, select **Issued** or **Issuing**. To search for both statuses, leave blank.
3. Click **Search**.

# Searching for an Identity

Use **Identity Search** to find an identity.

1. Fill out the following fields:
   - **Last Name** field.
   - (Optional) **First Name** and/ or **Internal Number** fields.
   - (Optional) **Group** field.

   Blank entries will return all identities.

   > **Note:** *Identities using SALTO devices only.* First Name and Last Name are required. *Identities using HID Origo tokens only.* First Name, Last Name, and Email Address are required to enroll the identity in HID Origo. *Identities using DMP intrusion panels.* Identities are defined by their DMP user name, ID and DMP panel name.

2. Add other search criteria.
   a. **Search Field** drop down list.
   b. **Search Value** field.
   c. Click **Add Criteria** to add another search field and value.

To clear all fields, click **Clear Search**.

To remove a search row, click **Remove**.

3. To the right of the **Search** button, select either:
   - **And** to find all identities that fit all entered criteria.
   - **Or** to find identities that fit one or more of the entered criteria.
4. Click **Search**.

   The page displays your search results.

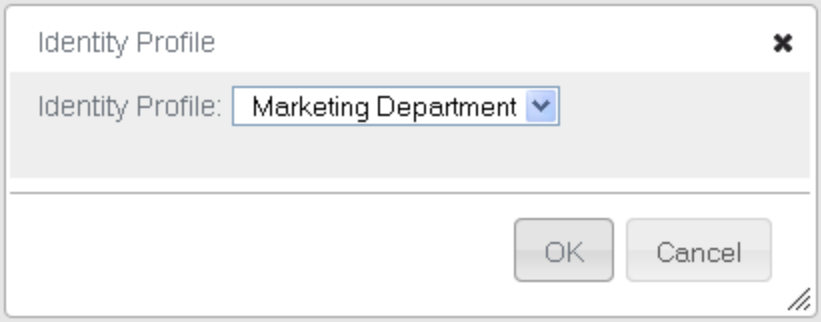
# Adding an Identity

A person with an identity record in ACM can be issued a badge to enter the physical site. A user of the ACM software can be issued a login and password.

To add a new identity:

1. Select **Identities**.
2. Click **Add Identity**.

   If Identity Profiles are configured, select the profile for the identity and click **OK**. The Identity Add page appears with the details of the identity profile. Otherwise, click **Cancel**.




3. Fill out the **Last Name** field and the required details.

   **Note:** Additional fields can be added using the User Forms or User Lists feature. *Identities using SALTO devices only.* First Name and Last Name are required. *Identities using HID Origo tokens only.* First Name, Last Name, and Email Address are required to enroll the identity in HID Origo.

4. Click **Save**.
5. Assign roles to the identity as required on the **Roles** tab and click .

   To add an item, select it from the **Available** list and click .

   To remove an item, select it from the **Members** list and click .

> **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

6. Enter the token details as required on the **Tokens** tab.

   By default the **Download** checkbox is selected, which downloads the token to the connected panels and associated doors. *Identities using SALTO devices only*. Click the **Download** button, which downloads the token to the SALTO server and door. *Identities using ASSA ABLOY IP devices only*. Click the **Download** button, which downloads the token to the DSR and door.

   When you are finished, click .
7. Optional: Add notes about the identity and review previous notes, if any.
8. Add more details about the identity on the following tabs:
   - **Roles**: Assigns a role to this identity.
   - **Tokens** : Creates a token for the identity.
   - **Groups**: Assigns the identity to a group.
   - **Capture**: Takes a photo of the user.
   - **Photos**: Uploads an existing photo of the user.
   - **Badge**: Assigns a badge to the user.
   - **Timed Access**: Assigns timed access to the user.
   - **Access**: View the identity's access privileges including roles, access groups and doors.
   - **Transactions**: View transactional data associated with the identity.
   - **Audit**: View a log of all the changes that have been made to this identity.

     The default Enrollment Operator role does not have access to this tab. Contact your System Administrator for more details.

> **Note:** The labels of the built-in tabs, such as Identity and Tokens, may be renamed by your System Administrator. A custom form or User Defined Tabs with User Defined Fields may be added at the end of the list.

# Assigning Roles to Identities

A role defines what a user has access to. For identities to have access to the system or physical access to the site, they must be assigned a role. Each role contains access groups and/or delegations. Access groups allow a user to have physical access to the site. Delegations allow a user to have access to the system. The user will be assigned a role depending on their position in the organization.

To assign roles to an identity:

1. Click **Identities**.
2. From the Identities Search page, perform a search for an identity.

   For more information, see *Searching for an Identity* on page 64.
3. Click on the name of the identity you want to edit.
4. Select the **Roles** tab.

5. From the Available list, select all the roles that you want to assign to the user, then click ►.
   The role is added to the Members list to show that it is now assigned.

   To remove a role from the user, select the role from the Members list, then click ◄.

   > **Note:** You can select multiple items by using the **Ctrl** or **Shift** key.

6. Click **Save**.

# Assigning Tokens to Identities

Tokens are used to authenticate individuals and allow or deny them physical access to your site. Tokens are assigned to personnel identity records along with access cards, biometric data such as fingerprints, or connected devices such as smartphones with apps that can be presented for authentication at readers.

To further restrict access, identities can be assigned to specific roles within your site.

To create tokens and assign them to an identity:

1. Select **Identities** > **Identities**.
2. Search for an identity.
   For more information, see *Searching for an Identity* on page 64.
3. Click the name of the identity you want to edit.
4. Select the **Tokens** tab.
5. If only one token has been defined, the Token: Edit page appears.
   If more than one token has been defined, the Tokens list appears. Click **Add Token**.
6. Enter the details as required.

   > **Note:** If you are assigning HID Origo tokens, see *Configuring HID Mobile Access® Credentials* on page 62.

7. Click and then to return to the identity search.
8. Click **Download** to download the token to the connected panels and associated doors.
9. To assign this token to a badge, select the **Badge** tab.
   From the **Badge Token** drop down list, select the internal number you want to assign to the badge.
10. Click .

# Assigning Groups to Identities

Groups are used to group physical and/or system components. Groups are assigned to identities primarily for batch updates. For example, if all the badges are close to expiry and they are assigned to the same group, the expiration date can be extended through a batch job.

To assign groups to an identity:

1. Click **Identities**.
2. From the Identities Search page, perform a search for an identity.

   For more information, see *Searching for an Identity* on page 64.
3. Click on the name of the identity you want to edit.
4. Select the **Groups** tab.
5. From the Available list, select all the groups that you want to add the user to, then click ▶.

   The group is added to the Members list to show that the user is now a member.

   To remove a user from a group, select the group from the Members list, then click ◀.

   > **Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

6. Click **Save**.

# Deleting a Token

To delete a token:

1. On the **Tokens** tab of an identity, click **Delete**.
2. Click **OK**.

# Capturing and Uploading Photos of an Identity

Capture or upload photos of a person from the **Photos** tab on a person's **Identity** page. Then you can select a photo from this page to appear on that person's Identity page or printed on an access badge.

**Captured photo**: A photograph taken by a badge camera connected to your computer and to the ACM system, and saved in the ACM system. Captured photos are in JPG format.

**Uploaded photo**: A graphics file in JPG, PNG, or GIF format that you upload from any location your computer can access and save in the ACM system. Typically, you would upload a JPG file for access badges.

> **Note:** The Microsoft Edge web browser supports only the uploading of JPG files. Do not attempt to upload any other file format if you are using the ACM client in the Microsoft Edge web browser. Using photos taken directly from a mobile phone is supported.

Photos saved in the ACM system can be cropped, resized, and rotated to meet the standardized requirements of the badge templates defined in your system.

You can use two types of cameras as a badge camera to capture a photo:

- **Local Camera** — Any camera connected directly to your computer or built into your computer or monitor.
- **IP-based camera** — Any IP-based camera previously connected to your network and added to your ACM system.

Before you can:

- Use a camera to capture photos, you must specify the badge camera you want to use in your user profile. For more information, see *External Systems - Defining the Badge Camera for the System* on page 414.
- Generate and print a badge, at least one badge template must be defined in your system.

After a photo has been added to the **Photos** tab of an identity, you can edit the photo to suit the requirements of your badge templates. Then you can create a badge with that photo. For more information, see *Creating Badges for Identities* on page 72.

**Capturing a photo**

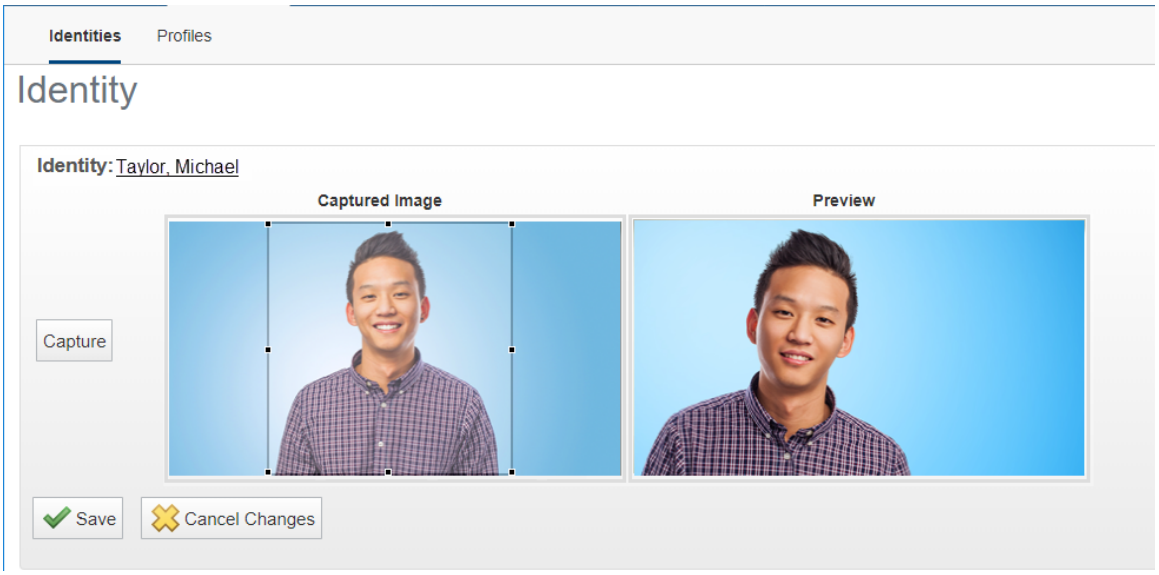
1. There are two ways to access the Capture page:
   - From the Identities Search page, click from the **Image Capture** column.
   - From the Identities Search page, click on the name of an identity, select the **Photos** tab, then click **Capture a Photo**.
2. If you are using:
   a. A local camera that you have not used before, this page will not appear unless you allow your web browser to access your camera. The first time you access the Capture page, you are prompted to allow your browser to access your local camera. Click **Allow**.
   b. An IP-based camera and the camera requires authentication, this page will not appear until you have entered your login credentials.

      Enter a user name and password, then click **OK**.

   The Capture page appears, with the live preview from the camera showing on the right.
3. Click **Capture**.

   The page refreshes to show the captured photo on the left and the live preview on the right.

   A cropping overlay is imposed over the photo, The aspect ratio of the overlay is determined by the values set on the **System Settings** page for **Badge Template Photo Height** and **Badge Template Photo Width**.




4. Click:
   - **Save** to save the photo that part of the image highlighted in the cropping overlay is saved. Cropping the photo using this aspect ratio ensures that the photo will fit exactly into the photo area on the badge without any distortion.
   - **Save and Edit** to save the photo and open the photo editing tool, or **Save** to add the photo directly to the **Photos** tab.
5. On the **Photos** tab, select the **Primary** checkbox if you want this photo to appear on this person's Identity page and access badge.
6. Click **Save**.

**Uploading a photo**

1. From the Identities Search page, click on the name of an identity, select the **Photos** tab, then click **Upload a Photo**.

   The screen expands to include more fields.
2. Click **Choose File** and navigate the directory to find the photo you want to upload.

   Click **Open** to select the photo. You can upload files in JPG, PNG, or GIF format.
3. On the **Photos** tab, click the **Primary** checkbox if you want this photo to appear on this person's Identity page and access badge. If no primary photo is selected, the first photo on the list is used.
4. Click **Save**.

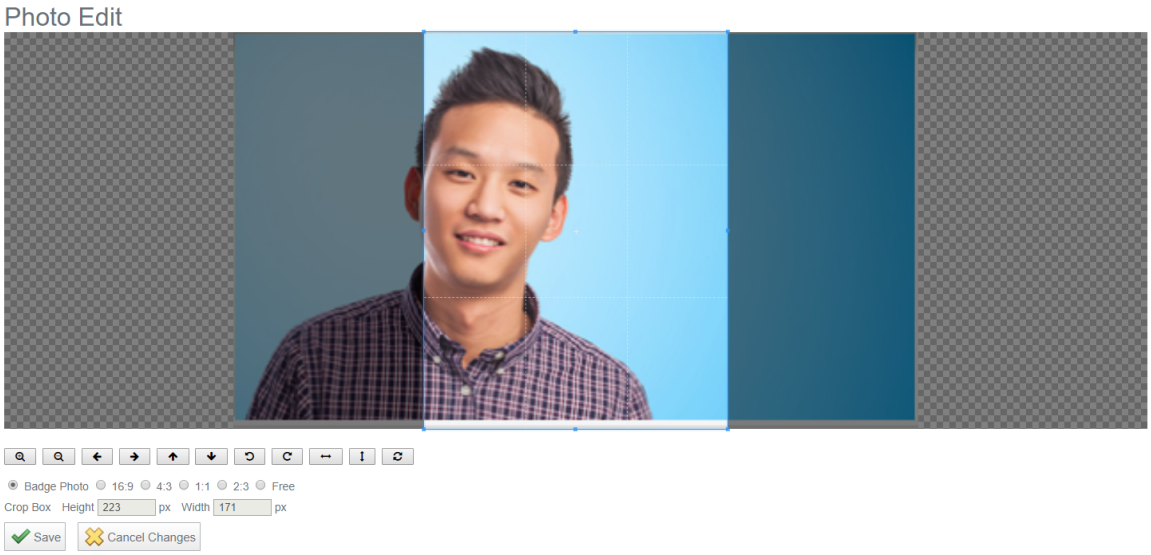
**Editing a photo**

You can edit a captured photo when you first save it by clicking **Save and Edit**. You can edit any saved photo by clicking on its filename link or thumbnail photo on the **Photos** tab.

The photo is displayed with a brighter cropping overlay imposed over it. The overlay is preset to the **Badge Photo** aspect ratio. This ratio is determined by the values set on the **System Settings** page for **Badge Template Photo Height** and **Badge Template Photo Width**. Cropping the photo using this aspect ratio ensures that the photo will fit exactly into the photo area on the badge without any distortion.

Use the mouse in combination with the control buttons under the photo to crop, resize, rotate and flip the photo. You cannot edit the actual photo, or change its resolution by zooming in and out. The dimensions

shown in the Crop Box options are read-only and cannot be entered directly, but are dynamically updated as you manipulate the cropping overlay with the mouse.




1. Adjust the overlay.
    - To reposition the overlay over the photo:
        a. Click inside the cropping overlay.
        b. Drag the mouse to move the overlay.
    - To resize the overlay
        a. Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay can be resized.
        b. Resize the overlay. The selected aspect ratio (usually the Badge Photo aspect ratio) is retained.
    - To change to a different aspect ratio:

      Click to select the required aspect ratio.
    - To resize the overlay freely:
        a. Click **Free**.
        b. Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay will be resized.
        c. Drag the mouse to resize the overlay. The overlay will be resized only in the direction of the cursor.
    - To rotate the overlay:
        a. Click outside the current overlay.
        b. Drag the mouse to draw a new overlay.
    - To replace the overlay:
        a. Click outside the current overlay.
        b. Drag the mouse to draw a new overlay.

2. Adjust the photo.
    - To enlarge or reduce the photo:

      Use the + and - magnifier control buttons to adjust the photo size in stepped increments.
    - To reposition the photo:

      Use the up, down, left and right control buttons to adjust the photo position in stepped increments.
    - To rotate the photo:
        a. Use the counterclockwise circular arrow to rotate the photo to the left by 90°.
        b. Use the clockwise circular arrow to rotate the photo to the right by 90°.
    - To flip the photo:
        a. Use the horizontal double-ended control button to flip the photo left to right.
        b. Use the vertical double-ended control button to flip the photo top to bottom.
    - To reset the photo:

      Use the reset control button to cancel your changes and revert the photo to its previously saved version.
3. Save the photo:

   Click **Save**.

   The **Photos** tab is displayed with the saved photo.

   When you save the photo, that part of the image highlighted in the cropping overlay is saved.

   > **Note:** The saved photo replaces the original photo. The original photo cannot be restored.

**Specifying the Primary photo**

If you have several photos saved on the **Photos** tab, the first photo is used on that person's Identity page and is selected by default for the access badge. To use another photo instead, select the **Primary** checkbox of the photo you want.

**Deleting a photo**

To delete a photo from the **Photos** tab:

1. Click .
2. Click **Save**.

# Creating Badges for Identities

Badges are identification cards that are used to verify a user's identity or association to an organization. Badges may also be used as access cards if they are printed directly on the person's RFID badge.

> **Note:** Before you can print a badge, you must connect a badge printer to the network and configure it. For instructions on how to configure your badge printer, refer to the printer's user guide.

To create a badge for a user:

1. Click **Identities**.
2. From the Identities list, click on the name of the identity you want to edit.
3. Select the **Badge** tab.
4. From the **Badge Photo** drop down list, select a photo for this badge.

   Only the photos that have been previously uploaded or captured for this identity appear in this list.
5. From the **Badge Token** drop down list, select the token you want to associate with this badge.

   Only the tokens that have been previously defined for this user appear in this list.
6. From the **Badge Template** drop down list, select the badge template that you want to use for this badge.

   Only the badge templates that have been previously defined appear in this list.
7. Click **Save**.
8. To print the badge, click **Create Badge**.

   The badge appears in a preview window.
9. Click **Print**.

**Note:** When printing the badge, ensure that the Header and Footer settings are turned off or set to blank.

# Timed Access

Timed access allows you to schedule access to a specific set of doors or access groups for one badge-holder identity. It is useful for providing temporary restricted access to your site for visitors, contractors, temporary employees, and so on.

Use timed access:

- By door to provide short-term restricted access to your site for visitors, contractors, temporary employees, and so on; for example, to allow a contractor to access only the doors needed to access the work site. Each timed access applied to a door adds a new access level to the panel attached to the door, and panels are restricted to a maximum of 254 access level entries. There is a risk that overuse of this feature without deleting entries can cause the number of access levels on a heavily used door, such as a front door, to exceed this maximum.
- By access group to provide groups of badge-holders access to specific areas for restricted times; for example to access canteen areas during meal hours, or parking garages during the working day. The risk of access levels accumulating is much reduced by using access groups.

**Note:** All timed access deletions must be done manually. There is no automatic clean-up of timed access entries.

**To find a timed access entry for an identity:**

1. Click **Identities**.
2. Search for the identity. For more detail refer to *Searching for an Identity* on page 64.
3. Click on the name of the identity. The Identity: Edit page displays.
4. Click on the **Timed Access** tab.

**To add a new timed access entry for an identity:**

1. Find the timed access entry for the identity.
2. Click on the **Timed Access** tab.
3. Complete the fields on the tab. Refer to the guidelines above to select the appropriate timed access type.
4. Click **Add**.

   The new timed access entry is added to the timed access list. If the timeframe for an entry is currently active it will display in green. Timeframes for timed access are not checked against schedules. If a timed access entry is displayed in green but is not working, check any related schedules.

**Note:** You cannot edit a timed access entry. To change the details of an entry, delete the timed access entry and add a new one.

**To delete a timed access entry for an identity:**

1. Find the timed access entry for the identity.
2. Click on the **Timed Access** tab.
3. View the timed access list.
4. Click ✖ to delete the related timed access entry.
5. Click **OK** when the message 'Are you sure you want to delete *<name>*' displays.

   The message 'Successfully deleted the timed access entry *<name>*' displays.

**Note:** All deletions must be done manually. There is no automatic clean-up of timed access entries.

## Adding Timed Access to an Identity

To add a new timed access entry for an identity:

1. Click **Identities**.
2. Search for the identity. For more information, see *Searching for an Identity* on page 64.
3. Click the name of the identity.
4. Click the **Timed Access** tab.

5. Complete the following fields:
    - Name
    - Type
    - Appliance
    - Available/Members
    - Start Day/Time
    - End Day/Time
    - Schedule (if doors are selected as the Type)
6. Click **Add**.

   The new timed access entry displays in the timed access list. If the timeframe for an entry is currently active it will display in green. Timeframes for timed access are not checked against schedules. If a timed access entry is displayed in green but is not working, check any related schedules.

## Editing Timed Access

There is no functionality to edit a timed access entry. If you want to change the details of an entry, then:

- Delete the timed access entry. For more detail, refer to *Deleting Timed Access* below.
- Add a new timed access entry. For more detail, refer to *Adding Timed Access to an Identity* on the previous page.

## Deleting Timed Access

To delete a timed access entry:

1. Click **Identities**.
2. Search for the identity. For more detail refer to *Searching for an Identity* on page 64.
3. Click on the name of the identity.
4. Click on the **Timed Access** tab.
5. View the timed access list.
6. Click ✖ to delete the related timed access entry.
7. Click **OK** when the message 'Are you want to delete *<name>*' displays.

   The message 'Successfully deleted the timed access entry *<name>*' displays.

**Note:** All deletions must be done manually. There is no automatic clean-up of timed access entries.

# Editing an Identity

An identity must be edited when user information changes. For example if a user changes roles, their identity would need to reflect this. If the role is not updated, the user would not be able to access areas required for their new role.

To edit an existing identity:

1. Click **Identities**.
2. Search on the Identity Search screen, then click on the identity you want to edit.
3. Optional: Add notes about the identity and review previous notes, if any.
4. Navigate through the tabbed pages and make the required changes.
   - **Identity:** The identity details.
   - **Roles**: Assigns a role to this identity.
   - **Tokens** : Creates a token for the identity.
   - **Groups**: Assigns the identity to a group.
   - **Capture**: Takes a photo of the user.
   - **Photos**: Uploads an existing photo of the user.
   - **Badge**: Assigns a badge to the user.
   - **Timed Access**: Assigns timed access to the user.
   - **Access**: View the identity's access privileges including roles, access groups and doors.
   - **Transactions**: View transactional data associated with the identity.
   - **Audit**: View a log of all the changes that have been made to this identity.

     The default Enrollment Operator role does not have access to this tab. Contact your System Administrator for more details.

**Note:** The labels of the built-in tabs, such as Identity and Tokens, may be renamed by your System Administrator. A custom form or User Defined Tabs with User Defined Fields may be added at the end of the list.

**Note:** Remember to click to save the changes on each page.

## Token Fields

Add or edit a token for an identity on the **Token** tab in **Identities**:

| | |
|---|---|
| **Token Type** | Displays only for ViRDI, PIV and PIV-I, SALTO, and HID Origo tokens:<br>• **Default**: For all other types of tokens.<br>• **VIRDI Biometrics**: Only if ViRDI system settings have been applied.<br>• **PIV** or **PIV-I**: Only if pivCLASS system settings have been applied. See *Appendix: pivCLASS Configuration* on page 503.<br>• **SALTO**<br>• **HID Origo** |

| | |
|---|---|
| **Mobile Application Type** | Displays only for **SALTO** tokens.<br><br>Default is **None**.<br><br>**JustIn Mobile** refers to the SALTO JustIN Mobile application that is installed on the mobile phone of the identity.<br><br>**Note:** When issuing mobile keys, the encoder requires access to the internet. |
| **Mobile ID Type** | Displays only for **HID Origo** tokens.<br>The mobile ID to be issued to the registered device. |
| **Mobile Phone Number** | Displays only for **SALTO** tokens.<br><br>The mobile phone number in international format (plus sign and no spaces).<br><br>+ country code, area code, phone number<br><br>Example: `+12345678910`<br><br>**Note:** The mobile app must be installed on the mobile phone of this phone number. |
| **User ID** | Displays for ViRDI Biometrics only; read-only field. The ID number for the token assigned from the range configured when the ViRDI external system was configured. |
| **Embossed Number** | The number to be printed on a badge.<br><br>Only required for physical access cards.<br><br>Does not display for ViRDI Biometrics and SALTO tokens. |
| **Internal Number** | The internal number that is assigned automatically to the token. This value is downloaded to panels to enable the token's access permissions.<br><br>**Note:** Duplicate numbers are not allowed in the ACM system. Ensure the configuration of mobile IDs in HID Origo prevents duplicate credential numbers.<br><br>Does not display for SALTO tokens. |
| **CHUID** | See *Appendix: pivCLASS Configuration* on page 503. |
| **PIN** | When a PIN is required, the PIN number that the user will be required to enter at a keypad card reader.<br><br>Does not display for ViRDI Biometrics tokens. |

| | |
|---|---|
| **Token Status** | The status of the token may be set manually and then updated by the system as follows:<br>• **Active**: The Not Yet Active token is set to Active when the current date is past the Activate Date.<br>• **Expired**: The Active token is set to Expired when the current date is past the Deactivate Date.<br>• **Inactive**: The Active token is set manually to Inactive without further update.<br>• **Not Yet Active**: The token is not active yet. |
| **Issue Level** | A number from 0 to 999999999, representing the issue level of the token.<br>Example: If a 3-digit length was configured on the Card Format: Edit page, you can enter 123 for the issue level of the card.<br>For more information, see *Issue Level Numbering for Reusing a Card Number* on page 307. |
| **Last Area** | The last area the token gained access to.<br>Does not display for SALTO tokens. |
| **APB Exempt** | A checkbox to exempt this token from anti-passback.<br>For more information, see *Anti-Passback Modes* on page 205.<br>Does not display for SALTO tokens. |
| **Trace** | A checkbox to enable the trace feature for the token. This will generate a trace event each time the token is used to gain access. The event can then be sent to monitoring, reported separately, and used in global I/O configurations.<br>Does not display for SALTO tokens. |
| **Download** | A checkbox to allow the token to be downloaded to connected panels. Default is enabled.<br>*SALTO tokens.* Click the **Download** button, which downloads the token to the SALTO server and door. |
| **Never Expire** | The token never expires. |
| **Extended Door Times** | A checkbox to give the token extended access time.<br>Once enabled, the door remains unlocked for a longer period of time than the standard access time to accommodate users that may require more time to enter a door.<br>Standard and extended access times are specified on the Door Edit page. |
| **Office** | Displays for SALTO tokens only.<br>A checkbox to enable the token to activate Office mode for a door that is configured for Office mode, which allows the cardholder to leave the lock open.<br>To use this mode, the cardholder presents the key to the door while pressing down the inner handle and repeats the procedure to undo the mode. |

| | |
|---|---|
| **Set Lockdown** | Displays for SALTO tokens only.<br><br>*SALTO standalone doors only.* A checkbox to enable lockdown mode for a door that has a lock that can support manual lockdown. For more information about lockdown in the SALTO system, refer to SALTO systems documentation.<br><br>To use this mode, the cardholder presents the key to the door's inside reader and repeats the procedure to undo the mode. |
| **Override Privacy** | Displays for SALTO tokens only.<br><br>A checkbox to allow the cardholder to access a door locked from the inside at any time. |
| **Override Lockdown** | Displays for SALTO tokens only.<br><br>A checkbox to allow the person to access a door closed from the inside during lockdown state. |
| **Audit Openings** | Displays for SALTO tokens only.<br><br>*SALTO standalone doors only.* A checkbox to audit the use of keys in standalone doors. Audits automatically occur in online doors. |
| **Enable Revalidation** | Displays for SALTO tokens only.<br><br>A checkbox to specify a period for revalidating a key before it becomes invalid. To make the token valid again, the cardholder can present the token to the online wall reader at any time.<br><br>For example, a key requires revalidation every seven days, if the update period is set to 7 days. If the key is used on the third day, the update period is reset. If the key is not used for over seven days, the key becomes invalid. |
| **Pin exempt** | A checkbox to exempt the token from PIN entry at a keypad card reader.<br><br>Does not display for SALTO tokens.<br><br>Not supported for ASSA ABLOY IP doors. |
| **Use/ Lose exempt** | A checkbox to prevent this token from expiring if you know the identity will return after an extended period of inactivity.<br><br>Does not display for SALTO tokens. |
| **Create Time Stamp** | When a token was issued to the mobile device of the identity. |
| **Issue Date** | The date the token was issued. Click the field to use the calendar. |
| **Activate Date** | The activation date for the token. Click the field to use the calendar. |
| **Deactivate Date** | The deactivation date for the token. Click the field to use the calendar.<br><br>In ACM 6.18 and later releases, there is no deactivate date for the token that has Never Expire enabled. |
| **Last Door** | The last door the token was used to gain access. |
| **Last Used** | The last time the token was used to gain access. |
| **1 free pass** | Displays when editing ViRDI Biometrics tokens only. From the drop-down list, select a door.<br><br>Click **1 free pass** to allow the user to enter the door without generating an APB error. |

| | |
|---|---|
| **Enroll** | Displays only for HID Origo tokens.<br>Sends an invitation email with app download instructions and invitation code in order that the identity can redeem the issued token.<br>**Note:** First Name, Last Name, and Email Address are required to enroll the identity in HID Origo. |
| **Issue Token** | Displays only for HID Origo tokens. Only applicable after the identity is enrolled.<br>Issues a mobile ID to the selected device. |
| **Send Invitation** | Displays only for HID Origo tokens.<br>Registers a new mobile device.<br>**Note:** After the invitation is accepted, issue a token to this device. |
| **Add Token** | Add another token. |
| **Save and Enroll** | Displays only for ViRDI Biometrics tokens. It is active when the Biometric Enrollment (BE) Manager is running.<br>Click the button to save your changes, and open the BE Manager to enroll and register the fingerprint for the identity.<br>**Note:** The button is grayed out when the connection to the BE Manager is no longer active:<br>Save and Enroll<br>When the connection to the BE Manager is re-established, the button is enabled automatically. A manual reload of the page is not needed.<br>(If your ACM client is running in a Chrome or Firefox web browser, and the BE Manager is running although this button is grayed out, you can initiate a connection by opening the URL https://avobiometric.loc:9875/ in your web browser.) |
| **Save** | Click this button to save your changes. |
| **Cancel Changes** | Click this button to discard your changes. |

**Delete**

Click this button to delete the token.

**Note:** The button is grayed out for ViRDI Biometrics tokens when the connection to the BE Manager is no longer active.

When the connection to the BE Manager is re-established, the button is enabled automatically. A manual reload of the page is not needed.

# Managing Roles

The Roles feature allows you to define the access control permissions and application permissions that are available in the system. After roles are defined they can be assigned to identities, depending on the type of access control or application functions they are permitted to have.

When you select Roles, the following options are displayed:

- **Roles** — Displays the Roles list, the starting page for this feature.
- **Policies** — Displays the Policies list.
- **Groups** — Displays the Groups list.
- **Access Groups** — Displays the Access Groups list.
- **Delegations** — Displays the Delegations list.
- **Partitions** — Displays the Partitions list.
- **Routing Groups** — Displays the Routing Groups list.
- **Elevator Access Levels** — Displays the Elevator Access Levels list.

## Configuring Roles

A role is a container for all the permissions an ACM operator needs in the ACM system to perform a specific function in the organization. Each role can include access groups, delegations, routing groups, and role-assignment privileges.

- An access group contains all the doors and elevator access levels that a badge holder needs to access.
- A delegation is a list of permissions for the functionality within the ACM system that allows an ACM operator to configure settings and monitor events.
- A routing group allows an ACM operator to monitor specific event types and hardware components.
- Within the role, you can also specify which roles an operator can assign to other people.

After you have defined access groups, delegations, routing groups, and role-assignment privileges, you can assign them to the appropriate roles, and then assign the roles to identities in the system.

### Adding a Role

A Role defines a set of permissions in the ACM application that allow users to perform specific functions.

> **Note:** Define your required access groups, delegations, and routing groups before you configure roles.

To add a new role:

1. Select **Roles** > **Roles**.
2. Click **Add Role** and enter a name for the new role.

   Or, click to create a copy of an existing role.

   > **Note:** A copy of a child role includes the link to the parent role. A copy of a parent role does not include any of the child roles.

3. Complete the remainder of the page with the required details.
4. Click **Save**.

   The Role Edit screen is displayed.
5. Select the **Access Groups** tab to assign access groups to the role.
6. Select the **Delegate** tab to assign delegations to the role.
7. Select the **Routing** tab to assign routing groups to the role.
8. Select the **Asgn Roles** tab to specify role-assignment privileges. Operators with this role can only assign the specified roles in this list to other people in the system.
9. Select the **Access** tab to view access groups, doors, and identities associated with this role.
10. Select the **Audit** tab to view a log of all the changes that have been made to this role.
11. Click **Save**.

## Editing a Role

To edit an existing role:

1. Click **Roles**.
2. From the Roles list, click on the role you want to edit.
3. Navigate through the tabbed pages and edit the details as required. The tabbed pages include:
   - Role Edit: use this page to edit general settings for the role.
   - Access Groups: use this page to assign access groups to the role.
   - Delegate: use this page to assign delegations to the role.
   - Routing: use this page to assign routing groups to the role.
   - Asgn Roles: use this page to specify role-assignment privileges. Operators with this role can only assign the specified roles in this list to other people in the system.
   - Access: use this page to view access groups, doors, and identities associated with this role.
   - Audit: use this page to view a log of all the changes that have been made to this role.

   > **Note:** Remember to click to save the changes on each page.

## Assigning an Access Group to a Role

You must assign an access group to a role to make it effective.

1. Select **Roles** > **Roles**.
2. Select the **Access Groups** tab.
3. Select the access groups that you want to add to the role.

   To add an item, select it from the **Available** list and click ►.

   To remove an item, select it from the **Members** list and click ◄.

   > **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

4. Click **Save**.
   All the people with the role now have the access permissions defined by the access group.

## Assigning Delegations to a Role

To assign delegations to a role:

1. From the **Roles** drop-down menu, select **Delegations**.
2. From the list of roles on the Delegations panel, click on the role you want to edit.
3. From the Available list, select all the delegations that should be part of the role then click ►.
   The delegation is added to the Members list to show that it is now part of the role.

   To remove a delegation from the role, select the delegation from the Members list and click ◄.

   > **Tip:** You can select multiple terms by using the **Ctrl** or **Shift** key and move them with one click.

4. Click **Save**.

## Assigning Routing Groups to a Role

To assign routing groups to a role:

1. Click **Roles**.
2. From the Roles  list, click on the role you want to edit.
3. Select the **Routing** tab.
4. From the Available list, select all the routing groups that should be part of the role, then click ►.
   The routing group is added to the Members list to show that it is now part of the role.

   To remove an routing group from the role, select the routing group from the Members list, then click ◄.

   > **Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

5. Click **Save**.

## Assigning Roles

The **Asgn Roles** tab allows you to authorize members of this role to assign specified roles to other users.

To specify these permissions:

1. Click **Roles**.
2. From the Roles list, click on the role you want to edit.
3. Select the **Asgn Roles** tab.
4. From the Available list, select all the roles you want to allow members of this role to assign to others, then click .

   The role is added to the Members list.

   To remove a role from the list, select the role from the Members list, then click .

   > **Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

5. Click **Save**.

## Deleting a Role

To delete an existing role:

> **Note:** Default roles cannot be deleted.

1. Select **Roles**.
2. From the Roles list, click beside the role that you want to delete.
3. When the confirmation message is displayed, click **OK**.

## Searching for Roles

View all the roles that have been configured in the ACM system on the **Roles** page.

To narrow down the search results:

1. Select **Name**, **Installed**, **Default**, **Never Expire**, **Start Date**, **Stop Date**, or **Partitions** in **Search Field**.

   **Partitions** is displayed only if partitions are defined in your ACM system.
2. Select the search operator in **Search Value** and your search criteria.
3. Optional. To refine your search, click **Add Criteria**, repeat the above steps, and select the **And** or **Or** search operator (located next to the Search button).

   To remove a single criteria row, click **Remove**. To clear all fields, click **Clear Search**.

4. Click **Search**.

The results are displayed.

| | |
|---|---|
| **Name** | The name of the role.<br>Click the name to edit the role. |
| **Parent** | The parent of the role.<br>Click the name to edit the role. |
| **Child Roles** | The child roles of the parent role. |
| **Installed** | The role is currently operational and available to the system, if enabled.<br>indicates it is disabled.<br>Click the icon to change the setting. |
| **Default** | The role is assigned automatically when adding a new identity.<br>indicates it is disabled.<br>Click the icon to change the setting.<br>**Note:** Changing this setting does not affect any existing identity. It is only applied when a new identity is created. For example, you can change these settings to enroll several identities with the same set of roles in a single session, or use them to define a common set of roles applicable to all identities. |
| **Start Date** | The activation date and time for the role. Default is today's date at time of role creation. |
| **Stop Date** | The deactivation date and time for the role; for example, `12/31/2037 23:59:59`. In ACM 6.18 onwards, there is no stop date for the role that has Never Expire enabled. |
| **Create a Copy** | Click to create a copy of an existing role.<br>**Note:** A copy of a child role includes the link to the parent role. A copy of a parent role does not include any of the child roles. |
| **Delete** | Click to delete the role from the database.<br>**Note:** Default roles cannot be deleted. |
| **Add Role** | Click the button to add a new role. |
| **Create New Report** | Click the button to generate a report of all the roles in the system. |

## Role Fields

Add or edit a role on the **Roles** > **Roles** page:

| | |
|---|---|
| **Name** | The name of the role. |
| **Parent** | The parent of the role.<br><br>Only the roles that have been defined in the system appear in the drop down list. The child role will inherit all the access permissions defined in the parent role. Also, you cannot delete a parent role until you delete all its children.<br><br>**Note:** This is an advanced feature and is only recommended for experienced operators. |
| **Start Date** | The activation date and time for the role. Default is today's date at time of role creation.<br><br>To use the calendar, click the field.<br><br>Date and time are displayed in the local time of the ACM appliance. |
| **Stop Date** | The deactivation date and time for the role; for example, `12/31/2037 23:59:59`.<br><br>To display the field and use the calendar, remove the checkmark in Never Expire before you click the field. In ACM 6.18 onwards, there is no stop date for the role that has Never Expire enabled.<br><br>Date and time are displayed in the local time of the ACM appliance. |
| **Never Expire** | The role never expires. For a new role, the setting is enabled by default. |
| **Installed** | The role is currently operational and available to the system, if enabled. |
| **Default** | The role is assigned automatically when adding a new identity.<br><br>Activating this setting does not affect any existing identity. It is only applied when a new identity is created. You will have to edit existing identities if you want this role applied to them. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Roles - Access Groups page

When select the **Access Groups** tab, the Access Groups page is displayed. Access groups are sets of physical access permissions including doors and elevator access levels. For more information on access groups, see *Managing Door Access* on page 105.

This page allows you to assign access groups to this role.

| Feature | Description |
|---|---|
| **Available** | A list of access groups that have been configured in the system.<br><br>To assign an access group to this role, select the access group, then click . |

| Feature | Description |
|---|---|
| **Members** | A list of access groups that have been assigned to this role.<br><br>To remove an access group from this role, select the access group, then click ◄ . |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

**Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

## Roles - Delegate page

When you select the **Delegate** tab, the Delegate page is displayed. Delegations are sets of permitted commands within the ACM application. For more information on Delegations, see *Managing Access in the Application* on page 110.

This page allows you to assign delegations to the role.

| Feature | Description |
|---|---|
| **Available** | A list of delegations that have been configured in the system.<br><br>To add a delegation to this role, select the delegation from the Available list, then click ► to move it to the Members list. |
| **Members** | A list of delegations that have been assigned to this role.<br><br>To remove a delegation from this role, select the delegation from the Members list, then click ◄ to move it to the Available list. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

**Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

## Roles - Routing page

When you select the **Routing** tab, the Routing page is displayed. Routing groups allow certain users to monitor specific event types and components during a specified time interval. For more information on Routing, see*Routing Events to the Monitor Screen* on page 119.

This page allows you to assign routing groups to the role.

| Feature | Description |
|---|---|
| **Available** | A list of routing groups that have been defined in the system.<br><br>To assign a routing group to this role, select the routing group, then click ▶ . |
| **Members** | A list of routing groups that have been assigned to this role.<br><br>To remove a routing group from this role, select the routing group, then click ◀ . |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

**Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

## Roles - Assign Roles page

When you select the **Asgn Roles** tab, the Asgn Roles page is displayed. This page allows you to specify which roles that members of this role can assign to other identities. For example, suppose you want to allow a Badge Administrator to assign roles for access rights to the facility. However, you might not want to allow a Badge Administrator to assign Super Admin or Monitoring Supervisor to a user.

| Feature | Description |
|---|---|
| **Available** | A list of roles that have been configured in the system.<br><br>To allow members of this role to assign a specific role to other identities, select the role, then click ▶ . |
| **Members** | A list of roles that the user is allowed to assign to others.<br><br>To remove a role from this list, select the role, then click ◀ . |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

**Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

## Roles - Access page

When you select the **Access** tab from the **Role**: **Edit** screen, a list of parent and child roles, identities, access groups, and doors associated with this role is displayed.

| Feature | Description |
|---|---|
| **Child Roles** | The child roles of the parent role.<br><br>Click **+** or **-** beside each role to show or hide the identities that are associated with that role. |

| Feature | Description |
|---|---|
| **Identities** | The identities that are members of the role. |
| **Parent** | The parent of the role.<br><br>Click **+** or **-** beside the parent role to show or hide the access groups and doors that are assigned to that role. |
| **Access Groups** | The access groups that are assigned to the role. |
| **Doors** | The doors that are assigned to the role. |

### Roles - Audit page

When you select the **Audit** tab, the Audit page is displayed, a log of all the changes that have been made to this role is displayed.

| Feature | Description |
|---|---|
| **Date** | The date and time when this role was modified. |
| **Operator** | The user that modified this role. |
| **Attribute** | The specific role detail that was modified. |
| **Before** | Identifies what the role detail was before it was modified.<br><br>If the cell is blank, there was no previous value. |
| **After** | Identifies what the role detail was changed to. |
| **Create New Report** | Click this button to create a PDF report with the details on this page. |

# Configuring Policies

Policies define access regulations for doors, inputs, and outputs. For example, you can specify the number of allowed PIN attempts at a keypad entry or the length of time a user is allowed to stay in an area. Use policies to override the settings that have been configured for individual doors, inputs, and outputs.

For doors, you can also define Priority Door policies for high-priority and emergency situations. A Priority Door Policy replaces the current settings for a group of doors, including settings applied by other door policies, priority and non-priority global actions, job specifications, and macros.

Priority-enabled policies are intended to support the emergency operating procedures at your site, including potentially life-threatening situations (such as fires, tornadoes, earthquakes, physical attacks), and hazardous situations (such as chemical spills, gas leaks, explosions). These policies require special permissions to configure, and use specific options to operate. For more information, see *Priority Situations* on page 438 and *Triggering Door Lockdown By Panic Button or Red Card* on page 447.

Policies are enabled through the Groups feature. After you have created a policy, you must assign it to a group of hardware components to make it effective. All users and security devices that are assigned to the group are affected by the policies that are in the group.

A policy is in effect when it is installed on the ACM appliance.

## Adding a Policy

To add a new policy:

1. Select **Roles** > **Policies**.
2. Click **Add New Policy**.

   The Policy Add page appears.
3. Fill out the **Name** field.
4. Select the hardware types that you want to override. The options include **Door**, **Input**, and **Output**.
5. Click **Save**.

   When the page refreshes, the Policy Edit screen is displayed.
6. Depending on the options you selected on the Policy Add page, this screen may have any of the following tabbed pages:
   - Select the **Mercury** tab to override settings for doors that are connected to a Mercury Security panel.
   - Select the **Input** tab to override settings for inputs.
   - Select the **Output** tab to override settings for outputs.

## Editing a Policy

To edit an existing policy:

1. Select **Roles** > **Policies**.

   The Policies  list appears.
2. Click on the policy you want to edit.

   The Policy Edit screen appears.
3. Navigate through the tabbed pages and make the required changes. Depending on the options you selected on the Policy Add page, this screen may have any of the following tabbed pages:
   - Mercury: use this page to configure a policy for doors that are connected to a Mercury Security panel.
   - Input: use this page to configure a policy for inputs.
   - Output: use this page to configure a policy for outputs.

   **Note:** Remember to click to save the changes on each page.

## Deleting a Policy

To delete an existing policy:

1. Select **Roles** > **Policies**.
2. From the Policies Listing page, click beside the policy that you want to delete.
3. When the confirmation message is displayed, click **OK**.

## Policies list

When you select **Roles** > **Policies**, the Policies  list is displayed. This page lists all the Policies that have been configured in the system.

| Features | Description |
|---|---|
| **Name** | The name of this policy.<br>Click the name to edit the policy details. |
| **Installed** | Indicates if this policy is communicating with the appliance. Yes ( ) or No ( ).<br>Click the icon to change the status. |
| **Door** | Indicates whether this policy affects doors. |
| **Input** | Indicates whether this policy affects inputs. |
| **Output** | Indicates whether this policy affects outputs. |
| **Delete** | Click to delete this policy from the database. |
| **Add New Policy** | Click this button to add a new policy. |
| **Create New Report** | Click this button to generate a report of all the policies in the system. |

## Policies - Policy Add page

When you click **Add New Policy** from the Policies list, the Policy Add page appears. Enter the required details.

| Feature | Description |
|---|---|
| **Name** | Enter the name of this policy. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Installed** | Check this box to indicate that this policy is currently operational and available to the system. |
| **Door** | Check this box to affect doors with this policy. |
| **Input** | Check this box to affect inputs with this policy. |
| **Output** | Check this box to affect outputs with this policy. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Policies - Policy: Add page

When you click on the **Policy** tab, the Policy Edit page is displayed. This page allows you to edit general policy settings.

Make any changes that may be required.

| Feature | Description |
|---|---|
| **Name** | Enter the name of this policy. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Installed** | Check this box to indicate that this policy is currently operational and available to the system. |
| **Door** | Check this box to affect doors with this policy. |
| **Input** | Check this box to affect inputs with this policy. |

| Feature | Description |
|---|---|
| **Output** | Check this box to affect outputs with this policy. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Policies - Mercury Security page

When you select the **Mercury** tab, the Mercury page is displayed. This page allows you to configure a policy that can be applied to a group of doors connected to a Mercury Security panel.

**CAUTION —** If no Door Mode is selected for this policy and you do not select a schedule or select Never Active and the policy is applied to a group of doors after a non-priority Global Action has been triggered, the Door Mode is set to Card Only regardless of the higher-priority setting applied by the Global Action.

| Field | Description |
|---|---|
| **Priority** | Click this checkbox to specify this is a Priority Door Policy. This option is only enabled when the values in the Lock Mode and Custom Schedule options are correctly configured.<br><br>The settings in a Priority Door Policy are applied to all Mercury Security doors and panels that the policy is associated with when it is activated. A Priority Door Policy is intended as a response to priority situations, such as unpredictable emergencies. For detailed instructions, see *Priority Situations* on page 438. |
| **Name** | Enter the name of this door policy. |
| **Access Type** | Select the access type for this door policy. |
| **Lock Mode** | For a wireless door, select the lock mode to be set by this door policy.<br><br>Select **None** if you are configuring a Priority Door Policy. This setting is used with the setting in the **Custom Schedule** option to enable the Priority checkbox. |
| **Door Mode** | Select the entry mode for the door when the door controller is online and communicating with the panel.<br><br>**Important:** You must select a Door Mode and for every door policy you create. If a Door Mode is not selected:<br>• The policy is not available to use for a Door Override.<br>• The Door Mode may be set to Card Only if the policy is installed after a non-priority Global Action has been triggered. |

| Field | Description |
|---|---|
| **Offline Door Mode** | Select the entry mode used for the door if the door controller is no longer communicating with the panel. The Offline Door Mode is no longer supported if the door controller is connected to an LP4502 panel that has replaced an HID VertX panel.<br><br>**Note:** In many cases readers in offline mode require a very simple solution for entry or exit because of the memory limitations. The recommended Offline Door Mode option is **Locked No Access**. |
| **Custom mode** | Select an additional door mode that will be active during the time specified in the **Custom Schedule** field. |
| **Custom Schedule** | Define when the Custom Mode would be active.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.<br><br>**Important:** Select **24 Hours Active** if you are configuring a Priority Door Policy. This setting is used with the setting in the **Lock Mode** option to enable the Priority checkbox. |
| **APB mode** | Select the Anti-Passback (APB) mode for this door policy.<br><br>For more information on Anti-Passback modes, see *Anti-Passback Modes* on page 205. |
| **APB delay** | Enter the number of seconds before another APB entry is allowed. |
| **Into Area** | Select the area that the user enters by passing through a door.<br><br>Only the areas that have been previously configured in the system appear in this list. |
| **Out of Area** | Select the area that the user exits by passing through a door.<br><br>Only the areas that have been previously configured in the system appear in this list. |
| **PIN timeout** | Enter the number of seconds that is allowed for a user to enter a PIN before it times out. |
| **PIN attempts** | Enter the number of times a user can attempt to enter a PIN before an Invalid PIN event is generated. |
| **LED mode** | Select the LED mode to specify how the reader LEDs are displayed.<br><br>For more information on LED modes, see *LED Modes for Mercury Security* on page 304. |
| **Held pre-alarm** | Enter the number of seconds a door can be held open before a pre-alarm is issued.<br><br>Instead of generating an alarm, it sends a warning signal to the Access Control Manager server. |
| **Access Time When Open** | Enter the number of seconds a door remains unlocked after access has been granted.<br><br>**Note:** This setting only applies, and must be configured, when the **Strike Mode** is set to **Full strike time**. |

| Field | Description |
|---|---|
| **Standard Access Time** | Enter the number of seconds a door remains unlocked after access has been granted.<br><br>If the door is not opened within this time, it will automatically lock.<br><br>**Note:** This time setting only applies, and must be configured, when the **Strike Mode** is set to **Cut short when open** or **Turn off on close**. |
| **Held open** | Enter the number of seconds a door can be held open before a Door Held Open event is generated. |
| **Extended access** | Enter the number of seconds a door remains unlocked after access has been granted to token holders with extended access permissions.<br><br>This feature is useful for users that may require more time to enter a door. |
| **Extended held** | Enter the number of seconds a door can be held open for users with extended access permissions.<br><br>This feature is useful for users that may require more time to enter a door. |
| **Strike Mode** | Select the strike mode.<br><br>• **Cut short when open** — The strike is deactivated when the door opens. This option requires that the door has a door position switch (DPOS) installed to monitor the **Open** and **Closed** door states. This strike mode is used with the **Standard Access Time** setting.<br>• **Turn off on close** — The strike is deactivated when the door closes. This option requires that the door has a DPOS installed to monitor the **Open** and **Closed** door states. This strike mode is used with the **Standard Access Time** setting.<br>• **Full strike time** — The strike is deactivated when the strike timer expires. This strike mode is used with the **Access time when open** setting. |
| **Mask Forced During** | Specify when Forced Door events are masked.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Mask Held During** | Specify when Door Held Open events are masked.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Always Mask Forced** | From the drop down box, select **TRUE** to mask all Forced Door events. |
| **Always Mask Held** | From the drop down box, select **TRUE** to mask all Door Held Open events. |
| **Door Processing Attributes** | |
| **Enable cipher mode** | Select **TRUE** to allow the user to enter their card number digits at the a keypad entry. |
| **Deny duress** | Select **TRUE** to deny access to a user that indicates duress at a door. |
| **Don't pulse door strike on REX** | Select **TRUE** to disable the pulse of the door strike when request-to-exit is activated.<br><br>For a policy for SimonsVoss wireless lock doors that do not support a door position switch (DPOS) , this box must be set to TRUE. |

| Field | Description |
|---|---|
| **Require two card control** | Select **TRUE** to specify that two tokens are required to open a door. This enforces two-person entry rule. |
| **Door forced filter** | Select **TRUE** to filter Forced Door events.<br><br>In case a door is slow to close or is slammed shut and bounces open for a few seconds, this filter allows three seconds for a door to close before generating an event. |
| **Log grants right away** | Normally, the system will log a single message for a card swipe and opened door. If you select **TRUE**, this will log two separate messages: one when access is granted and another when the door is opened. This event is not turned into an Access Control Manager event. |
| **Log all access as used** | Select **TRUE** to log all access grants regardless of whether or not the door was opened. |
| **Detailed events** | Select **TRUE** to generate detailed events of all hardware at the door including door position masking, timer expiration and output status.<br><br>This feature is useful for circumstances where it is important to know all the details of an event. |
| **Use shunt relay** | Select **TRUE** to enable the use of shunt relay for this door. |
| **Do not log Rex transactions** | Select **TRUE** to disable logging of request-to-exit transactions. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Create New Report** | Click this button to generate a PDF report on this door policy. |

## Policies - Input page

When you click the **Input** tab, the Input page is displayed. This page allows you to configure a policy for inputs.

| Feature | Description |
|---|---|
| **Name** | Enter the name of this input. |
| **Debounce** | Select the number of units (approximately 16 ms each) allowed for debouncing. |
| **Entry Delay** | Enter the number of seconds allowed for entry before this input issues an alarm. |
| **Exit Delay** | Enter the number of seconds allowed for exit before this input issues an alarm. |
| **Hold Time** | Set the amount of time that the alarm will stay in alarm after returning to normal.<br><br>For example, if the input point goes into alarm, then restores, it will hold it in that alarm state for 1 to 15 seconds after it returns to normal before reporting the normal state. |
| **Logging** | Enter the type of logging you need for this input. Valid values are:<br>• **Log all changes**: Log all changes affecting this input.<br>• **Do not log CoS if masked**: Log all changes except change of state events if the input is currently masked.<br>• **Do not log CoS of masked & no trouble CoS**: Log all changes except change of state events if the input is currently masked and there are no trouble CoS events. |

| Feature | Description |
|---|---|
| **Schedule** | Define when the input is masked. When the schedule is active, the input will be masked. |
| **Mode** | Enter the mode used for this input. The available options are:<br>• **Normal**: The door input is a normal door contact.<br>• **Non-latching**: The door input is a non-latching contact.<br>• **Latching**: The door input is latching contact. |
| **EOL resistance** | Select the EOL resistance value you need for this input.<br>Only those EOL resistance values previously defined for this system appear in this list. |
| **Enabled** | Check this box to indicate that this input is connected and ready to communicate with the Access Control Manager host. |
| **Masked** | Select TRUE to indicate that this input is normally masked. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Policies - Output page

When you click the **Output** tab, the Output page is displayed. This page allows you to configure a policy for outputs.

| Feature | Description |
|---|---|
| **Name** | Enter the name of the output. |
| **Enabled** | Check this box to indicate that this output is connected and ready to communicate with the Access Control Manager host. |
| **Mode** | Select the output mode. |
| **Pulse Time** | Enter the pulse interval time. This is the number of seconds that the output will activate when a pulse command is issued. This field is only available on outputs not associated with doors (e.g. auxiliary relays). |
| **Schedule** | Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Policies - Audit page

When you click the **Audit** tab, a log of all the changes that have been made to this policy is displayed.

| Feature | Description |
|---|---|
| **Date** | The date and time when this policy was modified. |
| **Operator** | The user that modified this policy. |
| **Attribute** | The field that was modified. |
| **Before** | The value in the field before this change took effect.<br>If this cell is blank, it indicates that there was no previous value. |
| **After** | The value in the field after this change took effect. |
| **Create New Report** | Click this button to generate a PDF of this audit history. |

# Configuring Groups

The groups feature allows you to group hardware components (cameras, doors, etc.) and/ or system components (identities, roles, etc.). Groups are useful for various functions, including:

- Applying identity profiles to many people at a time using the batch update feature.
- Applying door templates to many doors at once using the batch update feature.
- Enabling operators to monitor specific event types and hardware components through routing groups.
- Assigning policies to override settings on a group of hardware components.

**Note:** Groups should not be confused with Access Groups. For more information on Access Groups, see *Managing Door Access* on page 105.

## Adding a Group

To add a new group:

1. Select **Roles** > **Groups**.
2. Click **Add New Group**.
   The Group Add page appears.
3. Fill out the **Name** field.
4. Click **Save**.
   When the page refreshes, the Group Edit screen is displayed.
5. Navigate through the tabbed pages and edit the details as required. The tabbed pages include:
   - Group: use this page to rename the group and select partitions
   - Policies: use this page to assign policies to the group.
   - Members: use this page to add components to the group.
   - Audit: use this page to view a log of all the changes that have been made to this group.

## Editing a Group

To edit an existing group:

1. Select **Roles** > **Groups**.
   The Groups  list is displayed.
2. Click the name of the group you want to edit.
   The Group Edit page appears.
3. Navigate through the tabbed pages and make the required changes. The tabbed pages include:
   - Group: use this page to edit the group name and view the current policies and members in the group.
   - Policies: use this page to select the policies in the group.
   - Members: use this page to select the components in the group.
   - Audit: use this page to view a log of all the changes that have been made to this group.

**Note:** Remember to click to save the changes on each page.

## Assigning Policies to Groups

To assign policies to a group:

1. Select **Roles** > **Groups**.
   The Groups list is displayed.
2. From the Groups list, click on the name of the group you want to edit.
   The Group Edit page appears.
3. Select the **Policies** tab.
4. From the Available list, select all the policies that you want to assign to the group, then click .
   The policy is added to the Members list to show that it is now assigned.

   To remove a policy from the group, select the policy from the Members list, then click .

   **Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

5. Click **Save**.

## Assigning Members to Groups

A group can contain any number of members. Members of a group can be hardware items (cameras, doors, etc) and/or system items (identities, roles, etc).

To assign members to a group:

1. Select **Roles** > **Groups**.
   The Groups list is displayed.
2. From the Groups list, click on the name of the group you want to edit.
   The Group Edit page appears.
3. Select the **Members** tab.
4. From the **Type** drop down list, select the type of item you want to add to the group.
   Once you select a type, the relevant items will appear in the Available window.

   **NOTE**: If there are ten or more entries in the list in the Available window, a standard Search will display - this can be used to narrow the list. If there are more than 2,000 entries then an Advanced Search will display to enable you to narrow the list.

5. From the Available list, select all the items that you want to assign as members of the group, then click .
   The item is added to the Members list to show that it is now assigned.

To remove a item from the group, select the item from the Members list, then click ◄.

> **Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

6. Click **Save**.

## Creating a Hardware Group for Routing

To use routing groups, you must create a group that contains the event sources of interest. The event sources must be hardware components. For more information on routing groups, see *Routing Events to the Monitor Screen* on page 119.

1. Select **Roles** > **Groups**.

   The Groups  list is displayed.
2. Click **Add New Group**.

   The Group Add page is displayed.
3. Fill out the **Name** field.
4. Select a partition for the hardware group.

   This is important for routing if you do not want operators in different partitions to see this hardware group.
5. Click **Save**.

   The Group Edit screen is displayed.
6. Select the **Members** tab.
7. From the **Type** drop-down list, select a type of hardware component.

   > **Note:** Do not select **Identity** or **Role**, since they are not routable.
8. Select the hardware components that you want to add to the group.
9. Repeat the previous two steps if you want to add different types of hardware components to the group.
10. Click **Save**.

## Using Policies to Override Hardware Settings

1. Select **Roles** > **Policies**.
2. Create a policy. For more information on how to create a policy, see *Adding a Policy* on page 90.
3. Select **Roles** > **Groups**.

   The Groups  list is displayed.
4. Click **Add New Group**.

   The Group Add page appears.

5. Fill out the **Name** field, then click .
   When the page refreshes, the Group Edit screen is displayed.
6. Select the **Policies** tab.
7. Select the policy that you want to assign to the group, then click .
8. Select the **Members** tab.
9. From the **Type** drop-down list, select a type of hardware component.

   **Note:** Do not select **Identity** or **Role**, since they will not be affected by the policy.

10. Select the hardware components that you want to override, then click .
    The hardware in the group are now overridden by the specified policy.

# Performing an Identity Batch Update

The Batch Update feature allows you to assign an identity profile to many people at a time.

**Note:** You will need at least one identity profile and a group of identities to perform a batch update.

You can perform a batch update from either the Identity Profiles page or Groups page.

### Performing a Batch Update from the Identity Profiles page

1. Select **Identities** > **Profiles**.
2. On the Identity Profiles list, click in the **Batch Update** column beside the identity profile you want to apply.
   The Batch Update dialog box pops up.
   From the **Group** drop down list, select a group.
3. Click **OK**.
   All the identities in this group are updated with the identity profile.

### Performing a Batch Update from the Groups page

1. Select **Roles** > **Groups**.
2. From the **Batch Update** column, click beside the group that you want to edit.
   The Batch Update dialog box pops up.
3. From the **Identity Profile** drop down list, select an identity profile.
4. Click **Save**.
   All the identities in the group are updated with this identity profile.

# Performing an Identity or Template Batch Update

The Batch Update feature on the Roles page allows you to assign an identity profile to a group of identities,

or a door template to a group of doors from the same manufacturer. This is useful for applying new or modified standard settings to a group of identities or doors.

**WARNING —** There is a risk of losing a door template batch update report due to blocked pop-ups in your web browser. When a door template batch update is performed on a group of doors, a report is generated that you can save to your local system. If pop-ups from the ACM client are blocked by your web browser, the report cannot be saved. Your web browser will notify you that the pop-up is blocked, and offer you the option to unblock the pop-up. To save the report (and all future reports), you must enable pop-ups in your web browser from your ACM client. For instructions on how to enable pop-ups, refer to the Help files for your web browser.

1. Select **Roles** > **Groups**.

   The Groups  list is displayed.

2. From the **Batch Update** column, click beside the group of identities or group of doors that you want to update.

   The Batch Update dialog box pops up.

3. From the drop-down list, choose the identity profile or door template you want to apply to members of this group.

   Only the identity profiles or door templates previously defined by the system appear in this list.

4. Click **Save**.

   **Note:** If you are doing a door template batch update on a group of doors, you will either be prompted to save the report generated by the system (if pop-ups from the ACM client are unblocked) or your web browser will notify you that the pop-up has been blocked.

All members in this group now have the field values defined by the identity profile or door template.

## Scheduling an Identity or Door Batch Update

To schedule a batch update:

1. Select **Roles** > **Groups**.

   The Groups  list is displayed.

2. Click from the **Scheduler** column.

   The Job Specification - General dialog box displays.

3. Fill out the details as required.
4. Click **Next**.

   The Job Specification - Schedule dialog box displays.

5. From the drop down list, specify how often you want this update to occur.

   Depending on the value you select, additional fields appear.

6. Fill out the details as required.
7. Click **Next**.

   The Job Specification - Summary dialog box displays.

8. Click **Submit** to schedule this job.

   The job is scheduled.

# Deleting a Group

To delete an existing group:

1. Select **Roles** > **Groups**.
2. From the Groups list, click beside the group that you want to delete.
3. When the confirmation message is displayed, click **OK**.

# Groups list

When you select **Roles** > **Groups**, the Groups list is displayed. This page lists all the Groups that have been configured in the system.

| Feature | Description |
|---|---|
| **Name** | The name of this group.<br>Click the name to edit the group details. |
| **Members** | The number of members assigned to this group. |
| **Policy** | The number of policies assigned to this group. |
| **Batch Update** | Click to perform a batch update. |
| **Scheduler** | Click to schedule one or more batch updates. |
| **Delete** | Click to delete this group from the database. |
| **Add New Group** | Click this button to add a new group. |
| **Create New Report** | Click this button to generate a report of all the groups in the system. |

## Groups - Group Add page

When you click **Add New Group** from the Groups list, the Group Add page appears. Enter the required details in each tab.

| | |
|---|---|
| **Name** | Enter the name of this group. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Policies** | Select the policies that you want associated with this group. |
| **Members** | Select the members that you want associated with this group. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Groups - Group Edit page

When you click the **Group** tab, the Group Edit page is displayed. This page allows you to change the name of this group and view which policies and identities are currently associated with this group.

## Groups - Policies page

When you select the **Policies** tab, the Policies page is displayed. Policies are access regulations that you can

establish for doors, inputs, and outputs. For more information on policies, see *Configuring Policies* on page 90.

This page allows you to assign policies to this group.

| Feature | Description |
|---|---|
| **Available** | A list of policies that have been configured in the system.<br><br>To assign a policy to this group, select the policy from the Available list, then click ► to move it to the Members list. |
| **Members** | A list of policies that are currently associated with this group.<br><br>To remove a policy from the group, select the policy from the Members list, then click ◄ to move it to the Available list. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

**Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

## Groups - Members page

When you select the **Members** tab, the Members page is displayed. Groups can contain any number of hardware items (cameras, doors, etc) and/or system items (identities, roles, etc).

This page allows you to assign components to the group.

| Feature | Description |
|---|---|
| **Type** | Select the component type you want to add to this group.<br><br>Once you select a type, the relevant components will appear in the Available window. |
| **Available** | A list of available components in the system.<br><br>To assign an component to this group, select the component, then click ►. |
| **Members** | A list of components that are assigned to this group.<br><br>To remove a component from this group, select the component, then click ◄. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

**Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

## Groups - Audit page

When you click the **Audit** tab, a log of all the changes that have been made to this group is displayed.

| Feature | Description |
|---|---|
| **Date** | The date and time when this group was modified. |
| **Operator** | The user that modified this group. |
| **Attribute** | The field that was modified. |
| **Before** | The value in the field before this change took effect.<br><br>If this cell is blank, it indicates that there was no previous value. |
| **After** | The value in the field after this change took effect. |
| **Create New Report** | Click this button to generate a PDF of this audit history. |

# Managing Door Access

Access groups are sets of physical access permissions for doors and elevator access levels.

You must configure doors before you can create access groups. If you want to control access to the floors of a building, you should configure elevator access levels beforehand as well. For more information on elevator access levels, see *Managing Elevator Access* on page 124.

After you have created an access group, you must assign it to a role to make it effective. This allows members of the role to access the specified doors and elevator access levels in the access group.

## Adding an Access Group

To control access to the floors of your building, you must create elevator access levels. For more information, see *Managing Elevator Access* on page 124.

> **Tip:** It is recommended that you configure doors and elevator access levels before you create access groups.

To add a new access group:

1. Select **Roles > Access Groups**.
2. Click **Add Access Group** and enter a name for the new access group.

   Or, click to create a copy of an existing access group.

   > **Note:** A copy of an existing access group includes only the member's doors in your partition. The copy does not include any of the roles or identities that are associated with the existing access group.

3. Select an appliance to manage the access group.
4. Complete the remainder of the page.

   For more information, see *Access Group Fields* on page 109.
5. Click

**Save**.

The Access Group: Edit page is displayed.

6. Select the doors you want to add to the access group.

   To add an item, select it from the **Available** list and click ►.

   To remove an item, select it from the **Members** list and click ◄.

   > **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

7. Click **Save**.

   > **Tip:** If a message indicates the Advanced Schedule option cannot be enabled when saving, do any of the following:
   >
   > - Save the schedule without Advanced Schedule selected. Some doors only support basic schedules.
   > - Find the access groups using the schedule and select another schedule.

8. After you have created an access group, you must assign it to a role to make it effective. For more information, see *Assigning an Access Group to a Role* on page 83.

## Editing an Access Group

1. Select **Roles** > **Access Groups**.

   The Access Groups  list appears.

2. Click the name of the access group that you want to edit.

   The Access Group Edit page appears.

3. Navigate through the tabbed pages and make the required changes. The tabbed pages include:
   - Edit: use this page to edit the access group
   - Access: use this page to view the doors, roles, and identities that are in this access group
   - Audit: use this page to view a log of all the changes that have been made to this access group.

   > **Note:** Remember to click to save the changes on each page.

## Deleting an Access Group

> **Note:** You can only delete access groups that are not linked to any roles.

Before you can delete an access group, you must remove the access group from the associated role. For

more information, see *Assigning an Access Group to a Role* on page 83.

1. Select **Roles** > **Access Groups**.
   The Access Groups list is displayed.
2. From the Access Groups list, click beside the access group that you want to delete.
3. When the confirmation message is displayed, click **OK**.

## Access Groups - Example

Here is a scenario to exemplify the use of Access Groups: A user is assigned a role and a token. The assigned role may contain one or more access groups. Each access group specifies access permissions to one or more doors and panels during a certain time interval. When a token is downloaded, it receives access permissions to doors that have been specified by the role.

A working example is:

1. Create a role called "HR Role" that includes two access groups.
   - Access Group 1 has Schedule 9 am-5 pm M - F and Door "Front Door" on Panel 1.
   - Access Group 2 has Schedule 11 am-2 pm M - F and Door "Break Room Door" on Panel 2.
2. Assign a user to the HR Role.
3. Create a token for the user called Token A with the internal number 12345.

To download these access permissions to the appropriate panels, the program must perform these operations:

- Assign an access group to Panel 1 with a schedule of 9 am - 5 pm M - F and Door "Front Door". Name this Access Group 1.
- Assign an access group to Panel 2 with a schedule of 11 am - 2 pm M - F and Door "Break Room Door". Name this Access Group 2.
- Download Token A to Panel 1 - Token Number 12345, AG 1.
- Download Token A to Panel 2 - Token Number 12345, AG 2.

## Assigning an Access Group to a Role

You must assign an access group to a role to make it effective.

1. Select **Roles**.
2. In the Roles list, click the role you want to edit.
3. On the Role Edit page, select the **Access Groups** tab.
4. Select the access groups that you want to add to the role.

   To add an item, select it from the **Available** list and click .

   To remove an item, select it from the **Members** list and click .

   > **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

5. Click **Save**.
   All the people with this role now have the access permissions defined by the access group.

# Searching for Access Groups

View all the access groups that have been configured in the ACM system on the **Roles** > **Access Groups** page.

To narrow down the search results:

1. Select **Name**, **Schedule**, **Installed**, **Door**, or **Partitions** in **Search Field**.

   **Partitions** is displayed only if partitions are defined in your ACM system.
2. Select the search operator in **Search Value** and your search criteria.
3. Optional. To refine your search, click **Add Criteria**, repeat the above steps, and select the **And** or **Or** search operator (located next to the Search button).

   To remove a single criteria row, click **Remove**. To clear all fields, click **Clear Search**.
4. Click **Search**.

The results are displayed.

| | |
|---|---|
| **Name** | The name of the access group.<br>Click the name to edit the access group. |
| **Appliance** | The name of the appliance that manages the access group. |
| **Installed** | indicates the access group is communicating with the appliance.<br>indicates communication is disabled.<br>Click the icon to change the setting. |
| **Door** | The number of doors associated with the access group. |
| **Roles** | The roles that the access group is assigned to. |
| **Create a Copy** | Click to create a copy of an existing access group.<br>**Note:** A copy of an existing access group includes only the member's doors in your partition. The copy does not include any of the roles or identities that are associated with the existing access group. |
| **Delete** | Click to delete the access group.<br>**Note:** You cannot delete access groups that have been assigned to a role. |
| **Add Access Group** | Click the button to add a new access group. |
| **Create New Report** | Click the button to generate a report of all the access groups in the system. |

## Access Group Fields

Add or edit an access group from **Roles** > **Access Groups**:

| | |
|---|---|
| **Name** | The name of the access group. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Appliance** | The appliance that manages the access group. |
| **Schedule** | When the access group is active.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.<br><br>**Tip:** If a message indicates the Advanced Schedule option cannot be enabled when saving, do any of the following:<br>• Save the schedule without Advanced Schedule selected. Some doors only support basic schedules.<br>• Find the access groups using the schedule and select another schedule. |
| **Elevator Access level** | The elevator access level that applies to the access group.<br><br>Only the elevator access levels that have been defined in the system appear in this list. |
| **Installed** | If selected, the access group is currently operational and available to the system. |
| **Options** | **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.<br><br>**Privacy Override** *ASSA ABLOY IP-enabled door only.* Enables the cardholder to override and unlock a door that is locked from the inside after the privacy button has been pressed. |
| **Available** | The available doors on the appliance.<br><br>To add a door to the access group, select the door from the Available list and click ► to move it to the Members list. |
| **Members** | The doors that are assigned to the access group.<br><br>To remove a door from the access group, select the door from the Members list and click ◄ to move it to the Available list. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

## Access Groups - Access page

When you select the **Access** tab from the Access Group: Edit screen, a list of doors, roles and identities associated with this access group is displayed.

| Feature | Description |
|---|---|
| **Access Group** | The name of this access group.<br><br>Click the name to return to the Edit page. |
| **Doors** | A list of doors that can be accessed by identities in this access group. |
| **Roles** | A list of roles that are assigned to this access group.<br><br>Click **+** or **-** beside each role to show or hide the identities that are in the access group through the role. |
| **Identities** | A list of users that are members of the access group. |

### Access Groups - Audit page

When you select the **Audit** tab from the Access Group: Edit screen, a log of all the changes that have been made to this access group is displayed.

| Feature | Description |
|---|---|
| **Date** | The date and time when this access group was modified. |
| **Operator** | The user who modified this access group. |
| **Attribute** | The specific access group detail that was modified. |
| **Before** | Identifies what the access group detail was before it was modified.<br><br>If the cell is blank, there was no previous value. |
| **After** | Identifies what the access group detail was changed to. |
| **Create New Report** | Click this button to create a PDF report with the details on this page. |

# Managing Access in the Application

A delegation is a list of permissions to specific functionality within the ACM system that can be assigned to an ACM operator (or a group of operators) using roles. For example, you can create one delegation containing only the permissions that allow operators access to configure identity settings, and another delegations containing only the permissions that allow operators access to monitor events.

To give an ACM operator permission to use specific functions, you create a delegation that contains only the permissions to use those specific functions, and then assign that delegation to a role. Only when a role assigned that delegation s assigned to an operator can the operator access these functions. For example, for an operator to validate an SSL certificate from an LDAP server, that operator must be assigned a role that contains a delegation that includes the `Collaboration Validate Certificate` permission.

After you have created a delegation, you must assign it to a role to make it effective.

## Adding a Delegation

To add a new delegation:

1. Select **Roles** > **Delegations**.
2. Click **Add Delegation** and enter a name for the new delegation.

   Or, click to create a copy of an existing delegation.
3. Click **Save**.

   The Delegation Edit page appears.
4. Select the permissions you want to include in the delegation.

   To add an item, select it from the **Available** list and click .

   To remove an item, select it from the **Members** list and click .

   > **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.
5. Click **Save**.
6. After you have created a delegation, you must assign it to a role to make it effective. For more information, see *Adding a Delegation to a Role* below.

## Editing a Delegation

To edit an existing delegation:

1. Select **Roles** > **Delegations**.

   The Delegations list appears.
2. Click the name of the delegation you want to edit.

   The Delegation Edit page appears.
3. Make the required changes.
4. Click **Save**.

## Adding a Delegation to a Role

You must assign a delegation to a role to make it effective.

1. Click **Roles**.

   The Roles list is displayed.
2. From the Roles list, click on the role you want to edit.

   The Role Edit screen appears.
3. Select the **Delegate** tab.
4. Select the delegations that you want to add to the role.

   To add an item, select it from the **Available** list and click .

   To remove an item, select it from the **Members** list and click .

> **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

5. Click **Save**.
   All the people with this role now have the access permissions defined by the delegation.

## Deleting a Delegation

To delete an existing delegation:

1. Select **Roles** > **Delegations**.
   The Delegations list is displayed.
2. From the Delegations list, click beside the delegation that you want to delete.
3. When the confirmation message is displayed, click **OK**.

## Delegations list

When you select **Roles** > **Delegations**, the Delegations list is displayed. This page lists all the delegations that have been configured in the system.

| | |
|---|---|
| **Name** | The name of the delegation.<br><br>Click the name to edit the delegation. |
| **Members** | The number of tasks that are permitted in the delegation. |
| **Create a Copy** | Click to create a copy of an existing delegation. |
| **Delete** | Click to delete the delegation. |
| **Add Delegation** | Click this button to add a new delegation. |
| **Create New Report** | Click this button to generate a report of all the delegations in the system. |

### Delegations - Delegation: Edit page

When you click the name of a Delegation from the Delegations list, the Delegation: Edit page is displayed.

This page allows you to specify what tasks are authorized by this delegation.

| Feature | Description |
|---|---|
| **Name** | Enter the name of the delegation. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Available** | A list of available tasks in the ACM application.<br><br>To add a task to the delegation, select the term from the Available list, then click to move it to the Members list. |
| **Members** | A list of tasks that are Members of this delegation.<br><br>To remove a task from this delegation, select the term from the Members list, then click to move it to the Available list. |

| Feature | Description |
|---|---|
| **Search** | Enter a term, then click **Filter** to filter the results in the Available window.<br>Click **Clear** to remove the filter. |
| **Case-sensitive** | Check this box to indicate that the letters in the **Search** field are case-sensitive. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

**Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

# Managing a Partitioned ACM System

**Tip:** Refer to this information if you are performing initial configuration of an ACM appliance before its deployment.

Partitions are separate administrative access zones within the ACM system that can be independently managed. Since it is highly scalable, a single ACM system can be partitioned to manage access for individual tenants in an office tower, buildings on a campus, or locations in a geographically dispersed organization. Think of partitions as independent instances of an ACM system within your ACM system.

Partitioning is much like filtering. You can create simple functional partitions or complex special-purpose partitions. The more complex your partitioning is, the more carefully it needs to be administered.

**Note:** Do not confuse areas with partitions. A partition is a separate administrative access zone within the ACM system. An area is a physical location that requires additional access control. Therefore, in a partitioned system, an area is configured within a partition.

In a non-partitioned system, all the items and functions are potentially available to all identities (ACM operators and badge holders). Roles and delegations are used to restrict operator access to the functionality and items, and access groups are used to restrict badge holders physical access.

**Important:** In a partitioned system, all the items and functionality that are assigned to a partition are available only to identities who are also assigned to that partition. Within a partition, roles and delegations are used to restrict operator access to functionality and items, and access groups are used to restrict badge holders physical access. All partition items can be assigned to multiple partitions.

It is recommended that an ACM system is partitioned before it is deployed, and that you use the default

System Administrator identity (with the login ID **admin**) to set up the partitioned system.

Items not assigned to any partition belong to an unnamed partition, called the blank partition, and are available to all identities. Treat the blank partition as a separate partition that everyone can access. For badge holders, use the blank partition to contain the doors to common areas, which might include building entrances, parking garages, elevators, and the like, which all badge holders can access. For ACM operators, use the blank partition to contain the common items, which any operator can configure.

> **Tip:** Alternatively, you can create dedicated common partitions , which might be more practical for a geographically dispersed partitioned ACM system, and keep the blank partition empty.

When configuring an:

- Identity–Assigning an ACM operator to one or more partitions restricts the operator to items in their assigned partitions and those not assigned to any partition. Not assigning an operator to any partition restricts the operator to items not assigned to any partition.
- Item–Assigning an item to a partition restricts who can see or edit the item to ACM operators assigned to that partition. If you assign all partitions to an item, the item can be viewed by all operators EXCEPT those not assigned to any partition. If you do not select a partition, any ACM operator can edit the item.

After partitions are configured, the **Partition** drop-down menu appears as a configuration option for any object that can be assigned to a partition.

## Planning a Partitioned System

Ideally, plan how to partition your ACM system before you deploy it. It is much easier to deploy a partitioned system and then provision it than it is to add partitions to an already deployed system and reconfigure it all over again. If partitioning is not properly planned out and tested before it is operational, there is a risk that items may be hidden (inaccessible) to the users that need them to do their jobs properly.

Some of the considerations you should keep in mind when planning your partitions:

- Centralize control.

  Always use the default system administrator identity to set up partitions. This identity always has full access to all partitions.
- Limit ACM operator access to partitions.

  Only allow the ACM operators who are responsible for access control operations within a partition permission to access that partition. To enforce this:
  - Create a custom admin role for the ACM operator identities assigned to administer a partition. Configure this role and its delegations so that the system administrator of a partition is prevented from creating partitions or assigning themselves to other partitions.
  - Create custom roles with the required delegations for ACM operator identities assigned other responsibilities in a partition. Configure these roles to include only the delegations needed. The default roles (such as monitoring, or enrollment operator) can also be used, as they are preconfigured with the necessary delegations.

    For example, to create an enrollment operator who , ensure that
  - Create identity records for ACM operators restricted to specific partitions so that they cannot view or change their own identity records. Configure the operator's identity record (Identities>Identity) so that it is not visible to any partition that includes them as an operator (Roles>Partitions).

> **Important:** If you are partitioning roles or delegations, ensure that the operators assigned to those roles and delegations also have access to the partitions.

- Keep partitions as simple as possible.

  Avoid shared items within more than one partition. Ideally, set up each partition so that its physical infrastructure is completely separate from the other partitions. For example, no door should be in more than one partition. A partition should consist of only the items that need to be managed within that partition.

  Some examples are:

  - Doors and elevators shared by two tenants on the same floor. Create a separate partition for the shared doors and elevators and assign it to both tenants. The ACM operator for either tenant can configure the doors in that shared partition and each operator can allow badge holders to access doors in their own partition plus in the shared partition.
  - A geographically dispersed ACM system with remote offices. Create a partition for each remote office. The default system administrator can access all partitions and manage the entire system, and a local ACM system administrator at each remote office can manage their offices' partition. Badge holders who need access to more than one remote office can then be assigned to the partitions of the remote offices they need to access.

> **Tip:** If you must have partitions with duplicate items, such as doors shared by two tenants, be aware of some of the complications that administrators or other operators with access to some (but not all) partitions may encounter when modifying partitions. For example, you may experience problems if you have to change the configuration of your partitions as tenants move in or out, or increase or decrease their floorspace.

- Manage the blank partition carefully.

  The blank partition contains items not assigned to any partition.

  Any identity or item not assigned to a partition is defined by default to the blank partition, and is restricted to that partition. For example, badge holders restricted to the blank partition can only open doors in the blank partition. However, badge holders assigned to one or more partitions can open doors in the partitions to which they are assigned and in the blank partition. Similarly, ACM operators restricted to the blank partition can only configure items in the blank partition. However, operators assigned to one or more partitions can configure items in the partitions to which they are assigned and in the blank partition.

In a partitioned system, there will be a limited number of badge-holders who can access all the partitions, such as concierge, security, service, and maintenance personnel. These personnel should be assigned to all partitions in their identity record. Regardless of whether the system is partitioned, there should also be at least one other ACM operator assigned the SuperAdmin role, as a backup for the default System Administrator account for the ACM system.

## Configuring a Partitioned ACM System

It is recommended that you partition your ACM system before it is operational at your site, and that you use the default System Administrator identity (with the login ID **admin**) to set up the partitioned system.

Use the following workflow to set up your partitioned ACM system:

1. Determine how many partitions you need.
2. Create a custom delegation based on the Admin delegation that excludes the Identities New and Identities Edit delegations. For example Partition Admin Deleg.
3. Create a custom role that includes the new delegation. For example Partition Admin.
4. For each planned partition, create a new identity in the ACM system and assign it the Partition Admin role. This identity will be assigned to the partition as its local administrator.
5. Create each partition and add the identity of its local system administrator to the partition. Both the default system administrator and the local partition administrator identities can manage this partition.
6. Test the partitions you created before your ACM system is deployed. At the very least, each partition's ACM operators should enroll a sample set of badge holders and monitor them as they access the partitioned site.

After you have partitioned the system, you can use routing groups. For more information on routing groups, see *Routing Events to the Monitor Screen* on page 119.

## Adding a Partition

This is a basic procedure on how to add a partition. For a more advanced procedure on how to partition the ACM system, see *Configuring a Partitioned ACM System* on the previous page.

> **Tip:** It is recommended that you use the default Admin account to set up partitions.

To add a new partition:

1. Select **Roles** > **Partitions**.
   The Partitions  list is displayed.
2. Click **Add New Partition**.
   The Partition Add page appears.
3. Enter a name for the new partition, then click .
   The Partition Edit page appears.
4. Select the operators that you want to include in the partition.
   To add an item, select it from the **Available** list and click .
   To remove an item, select it from the **Members** list and click .

   > **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

5. Click **Save**.
   The **Partitions** field now appears as a configuration option for most system settings.

## Editing a Partition

To edit an existing partition:

1. Select **Roles** > **Partitions**.
   The Partitions  list appears.
2. Click the name of the partition you want to edit.
   The Partition Edit page appears.
3. Make the required changes.
   For a more advanced procedure on how to partition the ACM system, see *Configuring a Partitioned ACM System* on page 115.
4. Click **Save**.

### Deleting a Partition

To delete an existing partition:

1. Select **Roles** > **Partitions**.
2. From the Partitions  list, click  beside the partition that you want to delete.
3. When the confirmation message is displayed, click **OK**.

## Partitions -  List

When you select **Roles** > **Partitions**, the Partitions  list is displayed. This page lists all partitions that have been configured in the system.

| Feature | Description |
|---|---|
| **Name** | The name of this partition.<br>Click the name to edit the partition. |
| **Members** | The number of users that have access to this partition. |
| **Delete** | Click  to delete this partition. |
| **Add New Partition** | Click this button to add a new partition. |
| **Create New Report** | Click this button to generate a report of all the partitions in the system. |

### Partitions - Add page

To add a new partition:

1. Select **Roles** > **Partitions**.
2. Click **Add New Partition**.
   The Partition Add page appears.
3. Enter the name of this partition.
4. Click **Save**.
   The Partition Edit page appears.
5. From the Available list, select the users that should have access to the partition, then click .
   The users are added to the Members list to show that they have access to the partition.
   To remove users from the partition, select the users from the Members list and click .

> **Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

### Partitions - Partition Edit page

When you click the name of a Partition from the Partitions  list, the Partition Edit page is displayed.

This page allows you to add users to the partition.

| Feature | Description |
|---|---|
| **Name** | Enter the name of this partition. |
| **Available** | A list of users in the system. Only users with login credentials appear in this list.<br><br>To add a user to this partition, select the user from the Available list, then click ► to move it to the Members list. |
| **Members** | A list of users that have access to this partition.<br><br>To remove a user from this partition, select a user from the Members list, then click ◄ to move it to the Available list. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

> **Note:** You can select multiple terms by using the **Ctrl** or **Shift** key.

## Assigning Partitions to ACM Operators and Entities

After a partition (or a set of partitions) is created, populate each partition with the needed items for its deployment. Each partition should have:

- One or more ACM operators with specific responsibilities in that partition.

  Any identity with login credentials to the ACM system can be a member of a partition. Membership of an identity in a partition is assigned on the **Partition: Edit** page. For more information, see the *Partitions - Partition Edit page* above.

  If you do not want the operators in this partition to be viewed by other operators in the system, go to the Account Information section at the bottom of the Identity Edit page and assign them to the appropriate partition.
- These ACM operators must be assigned the roles and delegations that allow them access to the ACM system.

  You can use the default roles and delegations or create new ones. You can create roles and delegations like the default roles and delegations that are not assigned to any partition, which can be assigned to an operator in any partition. For example, you can create an identity record for an ACM operator responsible for enrolling other operators and badge holders in a specific partition. Assign the default enrollment operator role and its associated delegations to that identity record, and add that identity to the that partition.

  Alternatively, you can assign roles and delegations to specific partitions. Partitions are assigned to a

role on the Roles: Edit page, to a delegation ion the Delegation: Edit page.

> **Important:** If a role is assigned to specific partitions, operators not assigned to any of those partitions may be prevented from accessing the ACM system, or parts of it. To avoid this, ensure that all identities assigned the role also have access to the same partitions. You may also have to create additional roles to access the same functionality in the other partitions. The same is also true of delegations.

- All of the entities, such as doors and related infrastructure (policies, groups, access groups, routing groups, and elevator access levels), within the partition's scope that allow badge holders physical access to the site.

  Membership of any entity in a partition is assigned in its edit page. Navigate to the entity's edit page and select the partition, or partitions, from the **Partitions** drop-down list.

An empty, or blank, Partition field for any entity has a specific meaning. An entity not assigned to any partition can be viewed by all ACM operators, including those not assigned to a partition. However, as soon as any entity (which could be a badge holder, an operator, a door, or any logical entity such as an access group) is assigned to a partition, it can only be viewed by operators assigned to that partition. An entity assigned to more than one partition can be viewed by operators assigned to any of those partitions. When an entity is assigned to all partitions, it can be viewed by all operators except operators not assigned to any partitions.

For example, identity records with a blank partition field can be viewed by any ACM operator. However, identity records with one or more partitions assigned to them can only be viewed by ACM operators with access to any of those partitions. If you assign an ACM operator to a partition, their identity record can only be viewed by other operators assigned to that partition. Similarly, for badge holders assigned to a partition, their identity records can only be viewed by operators assigned to that partition and their access privileges are restricted to the reader and doors in that partition (plus readers and doors not in any partition).

# Routing Events to the Monitor Screen

A routing group controls which events are routed to an operator's Monitor screen. This is achieved by specifying event types and event sources in the routing group. Only those event types that originate from the specified event sources will be routed. This is an advanced feature that requires the use of partitions, groups, and roles, and should only be configured by an experienced operator.

For example, a lobby security guard may only need to monitor people who access the building through the front door during regular work hours, but they would not need to know about system activity in the ACM application. You can use a routing group to ensure that the security guard only sees events related to the lobby area.

You must set up partitions and groups before you can use routing groups. For more information on partitions, see *Managing a Partitioned ACM System* on page 113. For more information on groups, see *Configuring Groups* on page 98.

After you have created a routing group, you must assign it to a role to make it effective.

## Routing Groups - Introduction

A routing group controls which event types and event sources are routed to the Monitor screen.

For example, a lobby security guard may only need to monitor people who access the building through the front door during regular work hours, but they would not need to monitor operators that are logging in and out of the ACM application.

After you have defined a routing group, only the event types produced by the event sources during the specified schedule will be routed to the Monitor screen.

You must set up routing schedules and groups of hardware components before you can use routing groups.

## Adding a Routing Group

To add a new routing group:

1. Configure partitions for the routing group. For more information on configuring partitions, see *Configuring a Partitioned ACM System* on page 115.
2. Create a hardware group that contains the event sources of interest. For more information on creating a hardware group for routing, see *Creating a Hardware Group for Routing* on page 100.
3. If you want to route events for specific time intervals, set up one or more schedules. For more information on adding a schedule, see *Adding Schedules (Intervals in Schedules)* on page 377.
4. Select **Roles** > **Routing Groups**.

   The Routing Groups  list is displayed.
5. Click **Add New Routing Group**.

   The Routing Group Add page is displayed.
6. Enter a name for the routing group.
7. Complete the remainder of the page with the required details.

   **Important:** Select the appropriate partition for this routing group.

8. Click **Save**.
9. Select the **Event Types** tab.
10. Select the event types that you want to route.

    To add an item, select it from the **Available** list and click ►.

    To remove an item, select it from the **Members** list and click ◄.

    **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

    When you're finished, click .
11. Select the **Groups** tab.
12. Select the group of hardware components that you want to route.
13. Click **Save**.
14. After you have created a routing group, you must assign it to a role to make it effective. For more information, see *Assigning a Routing Group to a Role* on the next page.

## Editing a Routing Group

To edit an existing routing group:

1. Select **Roles** > **Routing Groups**.
   The Routing Groups list appears.
2. Click on the routing group you want to edit.
   The Routing Group Edit screen appears.
3. Navigate through the tabbed pages and make the required changes. The tabbed pages include:
   - Schedule: use this page to edit the routing group settings, including the name and schedule
   - Event Types: use this page to select the event types that you want to route
   - Groups: use this page to select the groups of event sources that you want to route

   **Note:** Remember to click to save the changes on each page.

## Assigning a Routing Group to a Role

You must assign a routing group to a role to make it effective.

1. Click **Roles**.
2. From the Roles list, click on the role you want to edit.
   The Role Edit screen appears.
3. Select the **Routing** tab.
4. Select the routing groups that you want to add to the role.

   To add an item, select it from the **Available** list and click .

   To remove an item, select it from the **Members** list and click .

   **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

5. Click **Save**.
   All the operators with this role can now monitor the events defined by the routing group.

## Deleting a Routing Group

To delete an existing routing group:

1. Select **Roles** > **Routing Groups**.
2. From the Routing Groups list, click beside the routing group that you want to delete.
3. When the confirmation message is displayed, click **OK**.

## Routing Groups list

When you select **Roles** > **Routing Groups**, the Routing Groups list is displayed. This page lists all routing groups that have been configured in the system.

| Feature | Description |
|---|---|
| **Name** | The name of the routing group.<br><br>Click the name to edit the routing group details. |
| **Schedule** | Indicates when this routing group is active. |
| **Event Type** | The number of event types that are in this routing group. |
| **Group** | The number of groups that are in this routing group. |
| **Delete** | Click to delete this routing group. |
| **Add New Routing Group** | Click this button to create a new routing group. |
| **Create New Report** | Click this button to generate a report of all the routing groups in the system. |

## Routing Groups - Add page

When you click **Add New Routing Group** from the Routing Groups list, the Routing Group Add page appears. Enter the required details.

| Feature | Description |
|---|---|
| **Name** | Enter the name of this routing group. |
| **Schedule** | Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Schedule Qualifier** | From the drop down list, select the option that qualifies the schedule.<br>• **Appliance** : Relative to the local time on the appliance when the transaction was created within the ACM system.<br>• **Event**: Relative to the local time when the originating event occurred. |
| **Installed** | Check this box to indicate that this routing group is currently operational and available to the system. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Routing Groups - Schedule page

When you click the name of a Routing Group from the Routing Groups list, the Routing Group Schedule page is displayed. Click on the **Schedule** tab to return to this page.

| Feature | Description |
|---|---|
| **Name** | Enter the name of this routing group. |
| **Schedule** | Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Schedule Qualifier** | From the drop down list, select the option that qualifies the schedule.<br>• **Appliance** : Relative to the local time on the appliance when the transaction was created within the ACM system.<br>• **Event**: Relative to the local time when the originating event occurred. |

| Feature | Description |
|---|---|
| **Installed** | Check this box to indicate that this routing group is currently operational and available to the system. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Routing Groups - Event Types page

When you select the **Event Types** tab from the Routing Group: Edit screen, the Event Types page is displayed. This page allows you to specify which event types should be routed in this routing group.

| Feature | Description |
|---|---|
| **Routing Group** | The name of this routing group.<br><br>Click this name link to return to the Schedule page. |
| **Available** | A list of event types configured in the system.<br><br>To add an event type to the routing group, select the term from the Available list, then click ► to move it to the Members list. |
| **Members** | A list of event types that are in this routing group.<br><br>To remove an event type from the routing group, select the term from the Members list, then click ◄ to move it to the Available list. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Routing Groups - Groups page

When you select the **Groups** tab from the Routing Group: Edit screen, the Groups page is displayed. This page allows you to add groups to this routing group.

| Feature | Description |
|---|---|
| **Routing Group** | The name of this routing group.<br><br>Click this name link to return to the Schedule page. |
| **Available** | A list of groups configured in the system.<br><br>To add a group to the routing group, select the term from the Available list, then click ► to move it to the Members list. |
| **Members** | A list of groups that are in this routing group.<br><br>To remove a group from the routing group, select the term from the Members list, then click ◄ to move it to the Available list. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

# Managing Elevator Access

An Elevator Access Level defines a badge holder's elevator access to the floors in a building.

For example, you can create an elevator access level that contains Floor 1 and Floor 3. When you add this elevator access level to an access group, all users in that access group will have access to Floor 1 and Floor 3.

If you want to control elevator access during specified time intervals, you must set up schedules prior to creating the elevator access level. For more information on schedules, see *Adding Schedules (Intervals in Schedules)* on page 377. After you have created an elevator access level, you must assign it to an access group to make it effective.

**Note:** This feature currently applies to Mercury Security elevator transactions in floor tracking mode.

## Adding an Elevator Access Level

If you want to control elevator access during specified time intervals, you must set up schedules prior to creating the elevator access level. For more information on schedules, see *Adding Schedules (Intervals in Schedules)* on page 377.

To add a new elevator access level:

1. Select **Roles** > **Elevator Access Levels**.
   The Elevator Access Levels listing page is displayed.
2. Click **Add New Elevator Access Level**.
3. Enter a name for the elevator access level in the **Description** field.
4. Select an appliance to manage the elevator access level.
5. Complete the remainder of the page with the required details.

5. Click **Save**.
6. After you have created an elevator access level, you must assign it to an access group to make it effective. For more information, see *Assigning an Elevator Access Level to an Access Group* below.

## Editing an Elevator Access Level

To edit an elevator access level:

1. Select **Roles** > **Elevator Access Levels**.
   The Elevator Access Levels Listing page appears.
2. Click on the elevator access level you want to edit.
   The Elevator Access Level Edit screen appears.
3. Make the required changes.
4. Click **Save**.

## Assigning an Elevator Access Level to an Access Group

You must assign an elevator access level to an access group to make it effective.

1. Select **Roles** > **Access Groups**.

   The Access Groups listing page is displayed.
2. Click the name of the access group you want to edit.
3. From the **Elevator Access Level** drop down list, select the elevator access level.
4. Click **Save**.

   All users in that access group now have access to the floors in the elevator access level.

# Deleting an Elevator Access Level

To delete an existing elevator access level:

1. Select **Roles** > **Elevator Access Levels**.
2. From the Elevator Access Level listing page, click beside the elevator access level that you want to delete.
3. When the confirmation message is displayed, click **OK**.

# Elevator Access Levels list

When you select **Roles** > **Elevator Access Levels**, the Elevator Access Levels list is displayed. This page lists all elevator access levels that have been configured in the system.

| Feature | Description |
|---|---|
| **Description** | The name of this elevator access level.<br><br>Click on the name to edit the elevator access level details. |
| **Delete** | Click to delete this elevator access level. |
| **Add New Elevator Access Level** | Click this button to add a new elevator access level. |

## Elevator Access Levels - Add page

When you click **Add New Elevator Access Level** from the Elevator Access Level list, the Elevator Access Level Add page appears. Enter the required details.

| Feature | Description |
|---|---|
| **Description** | Enter the name of this elevator access level. |
| **Appliance** | From the drop down list, select the appliance that manages this elevator access level. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Output** | Indicates the default output number. |
| **Description** | The name of each floor.<br><br>The floors are named by default, but you can rename them. |
| **Schedule** | Indicate when a card/code has free access to the specified floor, meaning a valid card/code is not required to access this floor.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |

| Feature | Description |
|---|---|
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

## Elevator Access Levels - Elevator Access Level: Edit page

When you click the name of an elevator access level from the Elevator Access Level  list, the Elevator Access Level: Edit page is displayed. Make any changes that may be required.

| Feature | Description |
|---|---|
| **Description** | Enter the name of this elevator access level. |
| **Appliance** | From the drop down list, select the appliance that manages this elevator access level. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Output** | Indicates the default output number. |
| **Description** | The name of each floor.<br><br>The floors are named by default, but you can rename them. |
| **Schedule** | Indicate when a card/code has free access to the specified floor, meaning a valid card/code is not required to access this floor.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

# Reports

The Reports screen allows you to create, edit, preview, and generate reports. Reports are used to gather information from the system in either a PDF or Spreadsheet. Reports can be saved on your local computer and referred to offline. For example, the Identity/Doors with Access Report can be used to view which doors each identity has access to. You have the option of using the default system reports or customizing the reports to fit your needs.

> **Note:** If you do not have the correct delegations, you may not be able to access some of the following pages. See your System Administrator for details.

## Generating Reports

Anytime you see **PDF** or **Spreadsheet**, you can generate and save a copy of the current report.

You can generate a copy of reports from the Reports list, the Report Edit page or from the Report Preview page.

Generated reports will only show the filtered information that is displayed. To edit the report before you generate it, see *Editing Reports* on the next page.

- Click to save the current report as a PDF file.
- Click to save the current report as a CSV format spreadsheet.

Most generated reports saved as PDF files contain a maximum of 2,000 records, except the Audit Log Report, which contains a maximum of 1,000 records. Reports saved as CSV format spreadsheet files contain a maximum of 2,000 records.

Depending on your web browser, the file may be auto-downloaded or you will be prompted to save the file to your local computer.

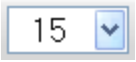
## Report Preview

When you click the name of a report from the Reports list and select , a preview of the selected report is displayed.

In the preview, you can check the report to see if the report gives you the information you need, search the report, or generate the report. For example, if you wanted to know the role of an identity, you can preview the Identity Summary report and search for the specific identity.

You can use the following options to control what is displayed:

**Tip:** Click to filter the report. The preview bar expands to display search criteria.

| Feature | Description |
|---|---|
| **Generate Report** | |
| The generate report options are displayed in the top left corner of the report preview. | |
| | Click this button to generate a PDF copy of the current report. |
| | Click this button to generate a CSV or spreadsheet copy of the current report. |
| **Preview Bar** | |
| The preview options are displayed at the bottom of the report page. | |
| | Click this icon to filter the report.<br>The report filter options are displayed. The options change depending on the report.<br>• Click **Search** to perform a search using the selected filter options.<br>• Click **Reset** to clear the report filter options.<br>• In the drop down list beside the Reset button, choose if the search will locate **all** or **any** transactions that match the selected report filters.<br>• Click **Save** to save and apply the selected filters to the default report. |
|   | Select the number of items you want to display on a single page. |
| | Click this button to return to the first page of the report. |
| | Click this button to return to the previous page of the report. |
| | Enter the page you want to go to. |
| | Click this button to bring up the next page of the report. |
| | Click this button to go to the last page of the report. |
| | Click this button to refresh the report. |

# Editing Reports

All reports can be edited or filtered to only display the information that you need. You can edit default system reports and custom reports in the same way.

If you plan to use the filtered report frequently, you can create a custom report rather than modify the default system report every time. For more information see *Creating Custom Reports* on page 130.

Most generated reports saved as PDF files contain a maximum of 2,000 records, except the Audit Log

Report, which contains a maximum of 1,000 records. Reports saved as CSV format spreadsheet files contain a maximum of 2,000 records.

Reports requiring more than 2,000 rows must be scheduled as a batch job for system performance. For more information, see *Generating a Batch Report* on page 456.

1. Display the Reports list.
   - To display the system reports page, click **Reports**.
   - To display the custom reports page, select **Reports** > **Custom Reports**.
2. Click for your report.

   **Note:** The Audit Log Report and Transaction Report do not have available. To edit, click on the report name and follow the steps in the related procedure - *Editing Audit Log and Transaction Reports* below.
3. Edit the report criteria.
4. Click to save your changes.

Now you can generate or preview the report with your changes.

# Editing Audit Log and Transaction Reports

The Audit Log and Transaction Reports are edited differently from other reports. There is no edit function directly available from the Reports list.

Follow the steps below to edit these reports.

1. Display the Reports list.
   - To display the system reports page, click **Reports**.
   - To display the custom reports page, select **Reports** > **Custom Reports**.
2. Click on the name of the report.
3. Click in the bottom left-hand corner on the following page (either the Grid: Transaction Report or Grid: Audit Log page).

   The Find section opens.
4. Do the following to define criteria for the report:
   - Select an option in the search type field (e.g. External System ID).
   - Select an option in the search operator field (e.g. greater or equal to).
   - Select an option in the search value field (e.g 12/07/2015 00:00:00).

   The **Full Name** search type field available for the Transaction Report returns results for a limited number of combinations of search operator and search value entries. For example, using an identity with the name John Smith, the following searches will succeed:

| Search Operator | Search Value |
|---|---|
| **contains** | Smith, John |
| | John |
| | Smith |
| **equal** | Smith, John |
| **begins with** | Smith |
| **ends with** | John |

5. Click to add more search fields, if required.
   Complete step 4 above for each additional field added.
6. Click **Save** to save your changes.
   The ACM Notification message displays with the message 'Search Parameters successfully changed'.
7. To save these filter settings as a custom report, enter a name in the Create Custom Report: field , then click **Create Custom Report:**.
8. To reset the search criteria, click **Reset**.

Now you can generate or preview the report with your changes.

# Creating Custom Reports

A custom report is a system report that has been duplicated and edited to meet your requirements. You can create a custom report that are used frequently.

1. Select **Reports** > **Reports**.
2. Click for the report you want to base the custom report on.
3. On the Report Edit page, select the **Copy Report** checkbox.
4. Give the new report a name.
5. Edit the report options to meet your requirements.
6. Click to save the new custom report.

See *Scheduling a Custom Report By Batch Job (Specification)* below.

# Scheduling a Custom Report By Batch Job (Specification)

To schedule the creation of a custom report by batch job:

1. Select **Reports** > **Custom Reports**.
2. Click the **Schedule** link next to the report name.
3. Create the schedule:
   a. In the Job Specification window with the report information, enter:

| | |
|---|---|
| **Name** | The name of the schedule. |
| **Output Format** | **pdf** (default) or **csv**. |

   b. Click **Next**.

      The current values of the report cannot be edited here. If you need to edit, go to the Custom Reports tab and click Edit.

   c. Enter the schedule:

| | |
|---|---|
| **Repeat** | **Once**, **Hourly**, **Daily**, **Weekly** or **Monthly**.<br>(The page refreshes depending on your selection.)<br>For Weekly: Any of the **Sun**, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat** checkboxes.<br>For Monthly: The date. |
| **On** | The time in 24-hour clock format in **HH** (hour, such as `20`) and **MM** (minute, such as `00`).<br>For Once: Click the field to select the date from the calendar. Then adjust the hour, minute and second selectors to set the time. |

   d. Click **Next**.
   e. Optional. Enter a checkmark in **Send Email** and the email address.

      If an email is not specified, go to the **Batch Jobs** tab to retrieve the report on the appliance (after the job specification completes).

   a. Click **Submit**. The schedule is created.
4. Create the batch job to run the custom report on schedule:
   a. Select > **My Account**.
   b. Click the **Job Specification** tab.
   c. Select the schedule and click **Activate/Deactivate**.

      The **Activated on** date is displayed in the right-most column.
5. To view the reports generated by the batch job, click the **Batch Jobs** tab. The reports stay in the list until manually deleted.

   To remove a report, select the row and click .

# Creating Custom Audit Log and Transaction Reports

A custom audit log report lists all the selected recorded system logs. You can create a custom audit log report to report only a selection of required audit logs. A custom transaction report lists all the selected recorded system transactions. You can create a custom transaction report to report only a selection of required system transactions.

1. Click **Reports**.
2. Click **Transaction Report** in the Report Name column.
3. Click at the bottom of the page. The preview bar expands to display search criteria.
4. Enter the details you want to include in the report in the Find section. (Click to add more fields.)
5. Click **Search**.
   The system transactions are filtered into a report.
6. In the **Create Custom Report** field, enter a name for the report.
7. Click **Create Custom Report** to save the new report.

# Physical Access

The Physical Access pages allow you to access all connected panels, doors, inputs, outputs and associated security devices. These devices can be added, modified, and deleted. The status of the hardware can also be monitored from these pages.

Panels are controllers that connect one or more door controllers (subpanels) and their associated readers to the appliance. Doors are logical units incorporating one or more components that are connected to a panel. The configuration of a door allows users to access certain areas.

Inputs are devices associated to panels and doors. For example, motion sensors or smoke detectors. Outputs are devices that perform tasks in response to input data. For example, unlocking a door or setting off a fire alarm.

**Note:** If you do not have the correct delegations, you may not be able to access some of the following pages. See your System Administrator for details.

## Templates Overview

For ASSA ABLOY, Avigilon and Mercury Security doors.

You can speed up the process of defining panels, subpanels and doors in the ACM system by creating templates for bulk creation. For example, door templates create doors that automatically populate field values on the Parameters and Operations tabs.

- Door templates

  Standardize door configurations that set the basic parameters and operational settings for each type of door at your site. Door templates are used when adding individual doors, modifying or updating common door settings for groups of doors, or when batch creating subpanels for doors when adding a new Mercury panel.

  **Note:** Only door templates are applicable to ASSA ABLOY doors.

  **Tip:** Although you can create multiple door templates with the same name, it is recommended that you give each the indoor template a unique name.

- Reader templates

  Standardize reader settings. Reader templates are referenced from a wiring template when batch creating subpanels for doors on a new panel.

- Output templates

  Standardize output settings. Output templates are referenced from a wiring template when batch creating subpanels for doors on a new panel, or used when batch creating output or input/output subpanels.

- Input templates

  Standardize input settings. Input templates are referenced from a wiring template when batch creating input subpanels for doors on a new panel, or used when batch creating output or input/output subpanels.
- Wiring templates

  Standardize Mercury subpanels with wiring templates that link subpanel addresses to door, reader, input, and output templates. Wiring templates are used to batch add the connections to functioning subpanels and doors wired to a new Mercury panel when the panel is added to the ACM appliance.

# Door Templates

A door template contains a predefined set of common parameter values and operational settings that can be applied to doors. Use a door template to populate the values assigned in the template to doors:

- When adding a new Mercury panel to the ACM system, new doors can be created in bulk by batch creating the subpanels on the new panel. Door templates are used together with wiring templates to create access-controlled doors with preset configurations ready for use after the new panel and subpanels are fully connected and communicating with the ACM system. To bulk create doors using a wiring template when adding a new panel, see *Batch Creating Subpanels on a New Mercury Panel* on page 161.
- When adding a new door, you still need to configure many attributes such as operations, hardware, cameras, and interlocks specifically for individual doors. To create a door using a template, see *Adding Doors* on page 214.
- When standardizing settings or updating settings supported by a door template for a group of doors.
  - When you have many doors defined with non-standard settings, create a group containing these doors and a new door template containing the standard settings. Then apply the new template to the group of doors.
  - When you have to change a setting common to all doors that use the same template, modify the door template. Then apply the modified template to the group of doors.

  You can apply a template to a group of doors:
  - Immediately from the Templates page, using the **Batch Update** option.
  - Alternatively, at any time after the template is created or modified, from the Groups using the **Batch Update** option.
  - At a future time, or on a schedule, from the Batch Jobs Specifications page.

  **Note:** When you use the **Batch Update** option and there are more than 10 doors in the group, a batch job is launched, which runs in the background.

To create a new template, see *Door Templates - Add page* on the next page.

When you select **Physical Access > Templates**, the **Door Templates** tab is selected, and the **Door Templates** list page is displayed. This page lists all door templates that have been defined in the system.

## Door Templates - Batch Update

The Batch Update feature on the Templates page allows you to assign a door template to a group of doors from the same manufacturer. This is useful for applying new settings or modifying current settings to a group of doors.

**WARNING —** There is a risk of losing a door template batch update report due to blocked pop-ups in your web browser. When a door template batch update is performed on a group of doors, a report is generated

that you can save to your local system. If pop-ups from the ACM client are blocked by your web browser, the report cannot be saved. Your web browser will notify you that the pop-up is blocked, and offer you the option to unblock the pop-up. To save the report (and all future reports), you must enable pop-ups in your web browser from your ACM client. For instructions on how to enable pop-ups, refer to the Help files for your web browser.

1. Select **Physical Access** > **Templates**.

   The Templates panel opens with the Door Template tab selected and the Door Templates list displayed.

2. On the Door Templates list, click from the **Batch Update** column beside the template you want to apply to a group.

   The Batch Update dialog box appears.

3. From the **Group** drop down list, select a group of doors.

   Only the groups that have been previously defined appear in this list.

4. Click **OK**.

   All members of the specified group are updated with this template's settings.

> **Note:** If you are doing a door template batch update on a group of doors, you will either be prompted to save the report generated by the system (if pop-ups from the ACM client are unblocked) or your web browser will notify you that the pop-up has been blocked.

If there are more than 10 doors, the update will be automatically scheduled as a batch job that starts two minutes after you select the group and click OK. This can be checked at > **My Account** > **Batch Jobs**.

## Door Templates list page

When you select **Physical Access** > **Templates**, the **Door Templates** tab is selected, and the **Door Templates** list page is displayed. This page lists all door templates that have been defined in the system.

| Feature | Description |
|---|---|
| **Name** | The name of the door template.<br>Click the name to edit the door template details. |
| **Batch Update** | Click to apply the template to all doors in a group. For more information, see *Door Templates - Batch Update* on page 139. |
| **Delete** | Click to delete the door template. |
| | Click to add a new door template. |

***Door Templates - Add page***

When you click:

- **Add Template** on the Door Templates list, the Templates: Add page appears. Enter the required door template details.
- On the name of a door template on the Door Templates list, the Templates: Edit page appears. All of the configurable items for a door that can be set using a door template appear in the Parameters and Operations tabs after you specify the vendor.

**Important:** To bulk add door subpanels when adding a new Mercury panel, you must use a door template that has a value specified for Door Mode. Before using the Subpanel: Batch Create wizard, ensure that a door template for the door subpanel type has been configured. Door templates without a Door Mode specified are not available for the wizard to use.

**Note:** You can add additional values to some drop down lists using the User Lists feature. For more information, see *Adding Items to a List* on page 390.

Name the template and specify the site and vendor information.

| Feature | |
|---|---|
| **Name** | You can change the name of the template. The name should be unique. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition.<br><br>The selection you make for the door template sets in which partitions doors are created. |
| **Vendor** | The name of the door manufacturer. After you select the name, the page is refreshed to show the Parameters tab. |
| **Model** | Select **Generic** for any vendor to display all the configurable items for that vendor's door controllers in the Parameters and Operations tabs. If you select Mercury as the Vendor, you can select the panel model. After you select the model, the page refreshes again to show only the configurable items for that model. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

After you select the vendor and model, update the individual items for the template to apply on the two panels on the **Parameters** tab:

- On the **Parameters** panel, for each item except Partitions, you can select from three or more choices, which vary from item to item:
  - <No Change>: Do not change the value. If the door is new, the item is left blank, or set to its default value. If there is already a value, it is unchanged.
  - <BLANK>: Clear the value. If the door is new, the item is left blank. If there is already a value, it is cleared. This choice only appears if no value is required.
  - All other choices are specific to that item.
  - The Partition item appears only if partitions are defined at your site.
- On the **Door Processing Attributes** tab, the choices are:
  - <No Change>
  - <Yes>
  - <No>

For detailed information about each item on the Parameters tab, see:

- *Parameters tab (Mercury Security)* on page 239
- *Parameters tab (VertX® )* on page 227

Next, update the individual items for the template to apply on the **Operations** tab:

- For the items with drop-down lists, except Card Formats, you can select from three or more choices, which vary from item to item:
    - <No Change>: Do not change the value. If the door is new, the item is left blank, or set to its default value. If there is already a value, it is unchanged.
    - <BLANK>: Clear the value. If the door is new, the item is left blank. If there is already a value, it is cleared. This choice only appears if no value is required.
    - For all the other items, enter a value in seconds, or leave blank to use the default value.
- For **Card Formats**, if you select:
    - <No Change>: Do not change the value. If the door is new, the list of card formats for the door will be populated by the card formats supported by the panel associated with the door.
    - <BLANK>: Clear the value. If the door is new, the list is left empty. If there is already a value, it is cleared.
    - Assign: Replace any card formats supported by the door with the card formats specified in the template.
    - Add: Append the card formats specified in the template to the card formats already supported by the door.
    - Remove: Remove the card formats specified in the template from the list of card formats supported by the door.

  After you make your choice of Assign, Add, or Remove, a list of all the configured card formats is displayed. Click to select one card format, or use any of click and drag, Shift and click, or Ctrl and click to select multiple card formats and move them to the Members list.

For detailed information about each item on the Operations tab, see:

- *Operations tab (Mercury Security)* on page 243
- *Operations tab (VertX®)* on page 229

***Door Templates - Door Template: Edit page***

When you click on the name of a door template on the Door Templates list, the Door Template: Edit page appears. All of the configurable items for a door that can be set using a door template appear in the Parameters and Operations tabs after you specify the vendor.

**Note:** You can add additional values to some drop down lists using the User Lists feature. For more information, see *Adding Items to a List* on page 390.

Name the template and specify the site and vendor information.

| Feature | |
|---|---|
| **Name** | Enter the name of the template. This field is required. The name should be unique. |

| Feature | |
|---|---|
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition.<br><br>The selection you make for the door template determines in which partitions doors are created. |
| **Vendor** | The name of the door manufacturer. After you select the name, the page is refreshed to show the Parameters tab. |
| **Model** | Select **Generic** for any vendor to display all the configurable items for that vendor's door controllers in the Parameters and Operations tabs. If you select Mercury as the Vendor, you can select the panel model. After you select the model, the page refreshes again to show only the configurable items for that model. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

After you select the vendor and model, update the individual items for the template to apply on the two panels on the **Parameters** tab:

- On the **Parameters** panel, for each item except Partitions, you can select from three or more choices, which vary from item to item:
  - <No Change>: Do not change the value. If the door is new, the item is left blank, or set to its default value. If there is already a value, it is unchanged.
  - <BLANK>: Clear the value. If the door is new, the item is left blank. If there is already a value, it is cleared. This choice only appears if no value is required.
  - All other choices are specific to that item.
  - The Partition item appears only if partitions are defined at your site.
- On the **Door Processing Attributes** tab, the choices are:
  - <No Change>
  - <Yes>
  - <No>

For detailed information about each item on the Parameters tab, see:

- *Parameters tab (Mercury Security)* on page 239
- *Parameters tab (VertX® )* on page 227

Next, update the individual items for the template to apply on the **Operations** tab:

- For the items with drop-down lists, except Card Formats, you can select from three or more choices, which vary from item to item:
  - <No Change>: Do not change the value. If the door is new, the item is left blank, or set to its default value. If there is already a value, it is unchanged.
  - <BLANK>: Clear the value. If the door is new, the item is left blank. If there is already a value, it is cleared. This choice only appears if no value is required.
  - For all the other items, enter a value in seconds, or leave blank to use the default value.

- For **Card Formats**, select <No Change>, <BLANK>, or specify the format to apply after choosing one of the following:
  - Assign: Replace any card formats supported by the door with the card formats specified in the template.
  - Add: Append the card formats specified in the template to the card formats already supported by the door.
  - Remove: Remove the card formats specified in the template from the list of card formats supported by the door.

  After you make your choice of Assign, Add, or Remove, a list of all the configured card formats is displayed. Click to select one card format, or use any of click and drag, Shift and click, or Ctrl and click to select multiple card formats and move them to the Members list.

For detailed information about each item on the Operations tab, see:

- *Operations tab (Mercury Security)* on page 243
- *Operations tab (VertX®)* on page 229

***Door Templates - Batch Update***

The Batch Update feature on the Templates page allows you to assign a door template to a group of doors from the same manufacturer. This is useful for applying new settings or modifying current settings to a group of doors.

**WARNING —** There is a risk of losing a door template batch update report due to blocked pop-ups in your web browser. When a door template batch update is performed on a group of doors, a report is generated that you can save to your local system. If pop-ups from the ACM client are blocked by your web browser, the report cannot be saved. Your web browser will notify you that the pop-up is blocked, and offer you the option to unblock the pop-up. To save the report (and all future reports), you must enable pop-ups in your web browser from your ACM client. For instructions on how to enable pop-ups, refer to the Help files for your web browser.

1. Select **Physical Access** > **Templates**.

   The Templates panel opens with the Door Template tab selected and the Door Templates list displayed.

2. On the Door Templates list, click from the **Batch Update** column beside the template you want to apply to a group.

   The Batch Update dialog box appears.

3. From the **Group** drop down list, select a group of doors.

   Only the groups that have been previously defined appear in this list.

4. Click **OK**.

   All members of the specified group are updated with this template's settings.

   > **Note:** If you are doing a door template batch update on a group of doors, you will either be prompted to save the report generated by the system (if pop-ups from the ACM client are unblocked) or your web browser will notify you that the pop-up has been blocked.

If there are more than 10 doors, the update will be automatically scheduled as a batch job that starts two minutes after you select the group and click OK. This can be checked at > **My Account** > **Batch Jobs**.

# Reader Templates

Use standardized reader settings and corresponding reader templates together with wiring templates to configure Mercury subpanels when adding panels in the ACM appliance. Standardize your reader configurations and create a reader template for each standard configuration in use at your site.

**Note:** Ensure all OSDP readers are configured in ACM software before physically connecting them.

OSDP is recommended for communications between readers, controllers and subpanels. OSDP offers support for bi-directional communication, Secure Channel Protocol (SCP) to encrypt the traffic, and provides additional status values for readers, improved LED controls, and simpler wiring.

Do not mix and match OSDP and non-OSDP readers on the same serial input/output (SIO) module. If OSDP is being used, set all all reader addresses (including unused ones) to OSDP to avoid accidental re-programming.

OSDP allows twice as many readers on most SIO modules. This allows a single controller port to control two OSDP readers, however the second reader only functions if both readers on the port use OSDP and the second reader is used on a paired door, or as the alternate reader for a single door. The second reader on an OSDP port cannot be used to create a second single door.

To access reader templates, select **Physical Access > Templates** and then click the **Reader Templates** tab. The **Reader Templates** list page is displayed. This page lists all reader templates that have been defined in the system.

**Tip:** After you have configured new doors using templates, you must access each door, panel, or subpanel to configure the unique settings that are not configured by each template.

## Reader Templates list page

When you select **Physical Access > Templates** and click the **Reader Templates** tab, the Reader Templates list page is displayed. This page lists all reader templates that have been defined in the system.

Ensure all OSDP readers are configured in ACM software before physically connecting them.

| Feature | Description |
|---|---|
| **Name** | The name of the reader template.<br>Click the name to edit the reader template details. |
| **Delete** | Click to delete the reader template. |
| | Click to add a new reader template. |

## Reader Template: Add page

When you click on the **Reader Templates** list page, the **Reader Template: Add** page appears. Enter the required reader template details.

**Note:** Ensure all OSDP readers are configured in ACM software before physically connecting them.

| Feature | Description |
|---|---|
| **Name** | Enter a  unique name for the template. |
| **Vendor** | Choose **Mercury Security** or **HID**. |
| **Mercury Security settings** | |
| **Reader Type** | Select the communication protocol used by readers configured with this template. The options include:<br>• **OSDP**<br>**Important:** A reader template for an OSDP reader defines the baud rate and the OSDP address to use. On a paired door using OSDP readers, you need four OSDP reader templates: one for each OSDP address.<br>OSDP is recommended for readers, controllers and subpanels communications. OSDP offers support for bi-directional communication, Secure Channel Protocol (SCP) to encrypt the traffic, and provides additional status values for readers, improved LED controls, and simpler wiring.<br>• **F/2F**<br>• **D1/D0 (Wiegand )**<br>• **CLK+Data (Mag)** ( NCI magnetic stripe standard)<br>• **Custom** (Default)<br>**Note:** The **Custom** option enables all options for all reader types. Readers configured with versions of the ACM software earlier than Release 5.10.4 are assigned this reader type when the software is upgraded to ensure that the previous settings are retained. |
| **The following options depend on the selected Reader Type and include:** | |
| **LED Drive** | Select the LED drive mode for readers configured with this template. The options depend on the reader model and how it is wired and include:<br>• **None**<br>• **Gen 1 wire**<br>• **Reserved**<br>• **Sep Red/Grn no buzz**<br>• **Dorado 780**<br>• **LCD**<br>• **OSDP** |
| **Format by nibble** | Check this box to indicate that readers configured with this template support the format by nibble. |

| Feature | Description |
|---|---|
| **Bidirectional** | Check this box to indicate that readers configured with this template can read bidirectionally. |
| **F/2F Decoding** | Check this box to indicate that readers configured with this template use F or 2F decoding. |
| **Inputs on reader** | Check this box to indicate that readers configured with this template provide one or more input ports for serial input arrays. |
| **Keypad decode** | Select the keypad decode/encryption method that is used by readers configured with this template. The options include:<br>• **MR20 8-bit tamper**<br>• **Hughes ID 4-bit**<br>• **Indala**<br>• **MR20 8-bit no tamper** |
| **Wiegand** | Check this box to indicate that readers configured with this template support the Wiegand standard. |
| **Trim Zero Bit** | Check this box to indicate that readers configured with this template support the trim zero bit standard. |
| **NCI magstripe** | Check this box to indicate that readers configured with this template supports the NCI standard for magnetic stripes. |
| **Supervised** | Check this box to indicate that readers configured with this template are supervised (outfitted with detection devices) |
| **Secure Channel Protocol** | Check this box to enable secure OSDP communication between the reader and the controller. The reader must support SCP and must be in installation mode. The reader will remain offline if a secure connection cannot be established.<br>**CAUTION —** Do not enable SCP on readers that support OSDPv1, such as the ViRDI biometric reader, as this will make the reader inoperable. Secure channel is only supported in by OSDPv2. |
| **Baud Rate** | Set the OSDP baud rate. This must be the same for all readers on a single port. Valid values are **9600** (default), **19200**, **38000** or **115200**. If blank is selected, the system will use default settings.<br>**Note:** Mercury controllers may auto-detect the OSDP baud rate. For more information, refer to Mercury documentation.<br>See *Appendix: pivCLASS Configuration* on page 503. |
| **OSDP Address** | Set the OSDP address. This must be different for each reader on a single port. Valid values are **0** (reader 1 default), **1** (reader 2 default), **2**, and **3**. If blank is selected, the system will use default settings.<br>**Note:** Mercury controllers will first try the setting provided and if that does not work, the controller will use default settings. |
| **OSDP Tracing** | Displayed for OSDP readers only. If the box is checked, OSDP address tracing will be logged in the `mercury.txt` appliance log for troubleshooting. |

| Feature | Description |
|---|---|
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **VertX® settings** | |
| **Keypad decode** | Select the keypad decode/encryption method that is used by readers configured with this template. The options include:<br>• **MR20 8-bit tamper**<br>• **Hughes ID 4-bit**<br>• **Indala**<br>• **MR20 8-bit no tamper** |
| **Wiegand** | Check this box to indicate that readers configured with this template support the Wiegand standard. |
| **NCI magstripe** | Check this box to indicate that readers configured with this template supports the NCI standard for magnetic stripes. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Reader Template: Edit page

When you click on the name of a template on the **Reader Templates** list page, the **Reader Template: Edit** page appears. Modify the required reader template details.

| Feature | Description |
|---|---|
| **Name** | Enter a  unique name for the template. |
| **Vendor** | Choose **Mercury Security** or **HID**. |
| **Mercury Security settings** | |

| Feature | Description |
|---|---|
| **Reader Type** | Select the communication protocol used by readers configured with this template. The options include:<br>• **OSDP**<br>**Important:** A reader template for an OSDP reader defines the baud rate and the OSDP address to use. On a paired door using OSDP readers, you need four OSDP reader templates: one for each OSDP address.<br>OSDP is recommended for readers, controllers and subpanels communications. OSDP offers support for bi-directional communication, Secure Channel Protocol (SCP) to encrypt the traffic, and provides additional status values for readers, improved LED controls, and simpler wiring.<br>• **F/2F**<br>• **D1/D0 (Wiegand )**<br>• **CLK+Data (Mag)** ( NCI magnetic stripe standard)<br>• **Custom** (Default)<br>**Note:** The **Custom** option enables all options for all reader types. Readers configured with versions of the ACM software earlier than Release 5.10.4 are assigned this reader type when the software is upgraded to ensure that the previous settings are retained. |
| **The following options depend on the selected Reader Type and include:** | |
| **LED Drive** | Select the LED drive mode for readers configured with this template. The options depend on the reader model and how it is wired and include:<br>• **None**<br>• **Gen 1 wire**<br>• **Reserved**<br>• **Sep Red/Grn no buzz**<br>• **Dorado 780**<br>• **LCD**<br>• **OSDP** |
| **Format by nibble** | Check this box to indicate that readers configured with this template support the format by nibble. |
| **Bidirectional** | Check this box to indicate that readers configured with this template can read bidirectionally. |
| **F/2F Decoding** | Check this box to indicate that readers configured with this template use F or 2F decoding. |
| **Inputs on reader** | Check this box to indicate that readers configured with this template provide one or more input ports for serial input arrays. |

| Feature | Description |
|---|---|
| **Keypad decode** | Select the keypad decode/encryption method that is used by readers configured with this template. The options include:<br>• **MR20 8-bit tamper**<br>• **Hughes ID 4-bit**<br>• **Indala**<br>• **MR20 8-bit no tamper** |
| **Wiegand** | Check this box to indicate that readers configured with this template support the Wiegand standard. |
| **Trim Zero Bit** | Check this box to indicate that readers configured with this template support the trim zero bit standard. |
| **NCI magstripe** | Check this box to indicate that readers configured with this template supports the NCI standard for magnetic stripes. |
| **Supervised** | Check this box to indicate that readers configured with this template are supervised (outfitted with detection devices) |
| **Secure Channel Protocol** | Check this box to enable secure OSDP communication between the reader and the controller. The reader must support SCP and must be in installation mode. The reader will remain offline if a secure connection cannot be established.<br>**CAUTION —** Do not enable SCP on readers that support OSDPv1, such as the ViRDI biometric reader, as this will make the reader inoperable. Secure channel is only supported in by OSDPv2. |
| **Baud Rate** | Set the OSDP baud rate. This must be the same for all readers on a single port. Valid values are **9600** (default), **19200**, **38000** or **115200**. If blank is selected, the system will use default settings.<br>**Note:** Mercury controllers may auto-detect the OSDP baud rate. For more information, refer to Mercury documentation.<br>See *Appendix: pivCLASS Configuration* on page 503. |
| **OSDP Address** | Set the OSDP address. This must be different for each reader on a single port. Valid values are **0** (reader 1 default), **1** (reader 2 default), **2**, and **3**. If blank is selected, the system will use default settings.<br>**Note:** Mercury controllers will first try the setting provided and if that does not work, the controller will use default settings. |
| **OSDP Tracing** | Displayed for OSDP readers only. If the box is checked, OSDP address tracing will be logged in the `mercury.txt` appliance log for troubleshooting. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **VertX® settings** | |

| Feature | Description |
|---|---|
| **Keypad decode** | Select the keypad decode/encryption method that is used by readers configured with this template. The options include:<br>• **MR20 8-bit tamper**<br>• **Hughes ID 4-bit**<br>• **Indala**<br>• **MR20 8-bit no tamper** |
| **Wiegand** | Check this box to indicate that readers configured with this template support the Wiegand standard. |
| **NCI magstripe** | Check this box to indicate that readers configured with this template supports the NCI standard for magnetic stripes. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

# Input Templates

Use standardized input settings and corresponding input templates together with wiring templates to configure Mercury subpanels when adding panels in the ACM appliance. Standardize your input configurations and create an input template for each standard configuration in use at your site.

To access input templates, select **Physical Access** > **Templates** and then click the **Input Templates** tab. The **Input Templates** list page is displayed. This page lists all input templates that have been defined in the system.

**Note:** Input templates for VertX® are not used by the ACM system. Input templates are only used when configuring Mercury subpanels.

**Tip:** After you have configured new doors using templates, you must access each door, panel, or subpanel to configure the unique settings that are not configured by each template.

## Input Templates list page

When you select **Physical Access** > **Templates** and click the **Input Templates** tab, the Input Templates list page is displayed. This page lists all input templates that have been defined in the system.

| Feature | Description |
|---|---|
| **Name** | The name of the input template.<br>Click the name to edit the input template details. |
| **Delete** | Click to delete the input template. |

| Feature | Description |
|---|---|
| | Click to add a new input template. |

## Input Template: Add page

When you click on the **Input Templates** list page, the **Input Template: Add** page appears. Enter the required input template details.

> **Note:** Input templates for VertX® are not used by the ACM system. Input templates are only used when configuring Mercury subpanels.

| Feature | Description |
|---|---|
| **Name** | The name of the template. |
| **Installed** | Check to indicate that input points configured with this template are connected and active. |
| **Vendor** | The only supported option is **Mercury Security**. |
| **Mercury Security settings** | |
| **Mode** | Select the mode used for arming and disarming the input to trigger alarm events. Each mode modifies the effect of the **Exit Delay** and **Entry Delay** settings.<br>• Normal – Does not use the **Exit Delay** and **Entry Delay** settings. Point is armed when the area is armed. Triggering the armed point will instantly trigger the alarm.<br>• Non-latching – Uses the **Exit Delay** and **Entry Delay** settings. When the area is armed, the point is armed after the time specified by the **Exit Delay** setting. This allows you time to exit the area without triggering an alarm. After the point is armed, triggering the armed point occurs after the time specified by the **Entry Delay** setting. This allows you time to disarm the area or restore the point (for example, by closing the door). This mode can be used in a scenario such as an armed fire door if you want people to exit but do not want the door propped open. The entry delay allows time for the door to be closed before triggering the alarm.<br>• Latching – Uses the **Exit Delay** and **Entry Delay** settings. When the area is armed, the point is armed after the time specified by the **Exit Delay** setting. This allows you time to exit the area without triggering an alarm. After the point is armed, triggering the armed point occurs after the time specified by the **Entry Delay** setting. This allows you time to disarm the area. |
| **EOL resistance** | Select the End of Line resistance value used by inputs configured with this template.<br>Only the EOL resistance values that have been defined in the system are listed. |
| **Debounce**[1] | Select how often the unit is allowed to debounce in a row. 1 = 16 ms, 2 = 32 ms, etc. |
| **Entry Delay** | The **Entry Delay** setting specifies the amount of time after you enter an alarmed area that you have to disarm the alarm system before an alarm is triggered.<br>Enter the number of seconds allowed before the input reports an event. |

[1]Due to mechanical properties of a switch, when a switch is closed, there is a period of time in which the electrical connection "bounces" between open and closed. To a microcontroller, this "bouncing" can be interpreted as multiple button pushes. To suppress the "bouncing", the controller software is designed to anticipate it. This is known as "debouncing a switch".

| Feature | Description |
|---|---|
| **Exit Delay** | The **Exit Delay** setting specifies the amount of time after the alarm system is armed that you have to leave the area without triggering an alarm.<br><br>Enter the number of seconds allowed before the input reports an event. |
| **Hold time** | Set the amount of time that the alarm will stay in alarm state after returning to normal.<br><br>For example, if the input point goes into alarm state, then restores, it will hold it in that state for 1 to 15 seconds after it returns to normal state before reporting the input point is in the normal state. |
| **Schedule** | Define when the input is masked. When the schedule is active, the input will be masked. |
| **Masked** | Check this box to indicate that this input is normally masked. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Show Policy** | Click this button to display the policies associated with this input module. |

## Input Template: Edit page

When you click on the name of a template on the **Input Templates** list page, the **Input Template: Edit** page appears. Modify the required reader template details.

> **Note:** Input templates for VertX® are not used by the ACM system. Input templates are only used when configuring Mercury subpanels.

| Feature | Description |
|---|---|
| **Name** | The name of the template. |
| **Installed** | Check to indicate that input points configured with this template are connected and active. |
| **Vendor** | The only supported option is **Mercury Security**. |
| **Mercury Security settings** | |

| Feature | Description |
|---|---|
| **Mode** | Select the mode used for arming and disarming the input to trigger alarm events. Each mode modifies the effect of the **Exit Delay** and **Entry Delay** settings.<br>• Normal – Does not use the **Exit Delay** and **Entry Delay** settings. Point is armed when the area is armed. Triggering the armed point will instantly trigger the alarm.<br>• Non-latching – Uses the **Exit Delay** and **Entry Delay** settings. When the area is armed, the point is armed after the time specified by the **Exit Delay** setting. This allows you time to exit the area without triggering an alarm. After the point is armed, triggering the armed point occurs after the time specified by the **Entry Delay** setting. This allows you time to disarm the area or restore the point (for example, by closing the door). This mode can be used in a scenario such as an armed fire door if you want people to exit but do not want the door propped open. The entry delay allows time for the door to be closed before triggering the alarm.<br>• Latching – Uses the **Exit Delay** and **Entry Delay** settings. When the area is armed, the point is armed after the time specified by the **Exit Delay** setting. This allows you time to exit the area without triggering an alarm. After the point is armed, triggering the armed point occurs after the time specified by the **Entry Delay** setting. This allows you time to disarm the area. |
| **EOL resistance** | Select the End of Line resistance value used by inputs configured with this template.<br>Only the EOL resistance values that have been defined in the system are listed. |
| **Debounce**[1] | Select how often the unit is allowed to debounce in a row. 1 = 16 ms, 2 = 32 ms, etc. |
| **Entry Delay** | The **Entry Delay** setting specifies the amount of time after you enter an alarmed area that you have to disarm the alarm system before an alarm is triggered.<br>Enter the number of seconds allowed before the input reports an event. |
| **Exit Delay** | The **Exit Delay** setting specifies the amount of time after the alarm system is armed that you have to leave the area without triggering an alarm.<br>Enter the number of seconds allowed before the input reports an event. |
| **Hold time** | Set the amount of time that the alarm will stay in alarm state after returning to normal.<br>For example, if the input point goes into alarm state, then restores, it will hold it in that state for 1 to 15 seconds after it returns to normal state before reporting the input point is in the normal state. |
| **Schedule** | Define when the input is masked. When the schedule is active, the input will be masked. |
| **Masked** | Check this box to indicate that this input is normally masked. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Show Policy** | Click this button to display the policies associated with this input module. |

[1]Due to mechanical properties of a switch, when a switch is closed, there is a period of time in which the electrical connection "bounces" between open and closed. To a microcontroller, this "bouncing" can be interpreted as multiple button pushes. To suppress the "bouncing", the controller software is designed to anticipate it. This is known as "debouncing a switch".

# Output Templates

Use standardized input settings and corresponding output templates to use together with wiring templates to configure Mercury subpanels when adding panels in the ACM appliance. Standardize your output configurations and create an output template for each standard configuration in use at your site.

To access output templates, select **Physical Access** > **Templates** and then click the **Output Templates** tab. The **Output Templates** list page is displayed. This page lists all output templates that have been defined in the system.

**Note:** Output templates for VertX® are not used by the ACM system. Output templates are only used when configuring Mercury subpanels.

**Tip:** After you have configured new doors using templates, you must access each door, panel, or subpanel to configure the unique settings that are not configured by each template.

## Output Templates list page

When you select **Physical Access** > **Templates** and click the **Output Templates** tab, the Output Templates list page is displayed. This page lists all Output templates that have been defined in the system.

| Feature | Description |
|---|---|
| **Name** | The name of the output template.<br>Click the name to edit the output template details. |
| **Delete** | Click to delete the output template. |
| | Click to add a new output template. |

## Output Template: Add page

When you click on the **Output Templates** list page, the **Output Template: Add** page appears. Enter the required output template details.

**Note:** Output templates for VertX® are not used by the ACM system. Output templates are only used when configuring Mercury subpanels.

| Feature | Description |
|---|---|
| **Name** | The name of the template. |
| **Installed** | Check to indicate that input points configured with this template are connected and active. |
| **Vendor** | The only supported option is **Mercury Security**. |

| Feature | Description |
|---|---|
| **Operating Mode** | Select how the panel knows when the output point is active.<br>• **Energized When Active** – a current is expected to pass through the output point when it is *active*.<br>• **Not Energized When Active** – a current expected to pass through the output point when it is *inactive*. |
| **Pulse Time** | Enter the pulse interval time. This is the number of seconds that the output will activate when a pulse command is issued.<br>**Note:** This field is only available on outputs not associated with doors (e.g. auxiliary relays). |
| **Schedule** | Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Output Template: Edit page

When you click on the name of a template in on the **Output Templates** list page, the **Output Template: Edit** page appears. Modify the required reader template details.

**Note:** Output templates for VertX® are not used by the ACM system. Output templates are only used when configuring Mercury subpanels.

| Feature | Description |
|---|---|
| **Name** | The name of the template. |
| **Installed** | Check to indicate that input points configured with this template are connected and active. |
| **Vendor** | The only supported option is **Mercury Security**. |
| **Operating Mode** | Select how the panel knows when the output point is active.<br>• **Energized When Active** – a current is expected to pass through the output point when it is *active*.<br>• **Not Energized When Active** – a current expected to pass through the output point when it is *inactive*. |

| Feature | Description |
|---|---|
| **Pulse Time** | Enter the pulse interval time. This is the number of seconds that the output will activate when a pulse command is issued.<br><br>**Note:** This field is only available on outputs not associated with doors (e.g. auxiliary relays). |
| **Schedule** | Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Wiring Templates

Use standardized wiring setups for your subpanels and corresponding wiring templates to speed up configuration of Mercury subpanels when adding managed doors to the ACM appliance. A wiring template corresponds to a standard wiring setup for the doors connected to a specific Mercury subpanel model.

A wiring template takes information from the door, input, output, and reader templates that you specify and validates all the information so that the template can be used to batch create subpanels configured with functional doors and readers.

Wiring templates use the Access Type options Single and Paired to support easier configuration of doors. Use Single for a door with one reader on one side of the door only (single reader door). Use Paired for a door with two readers, one on each side of the door (paired reader door). Paired readers allow each side of a single physical door to act like a separate door. This is particularly useful for antipassback and mustering.

The Access Type can also be configured in the Door Template. When configured in both the Wiring Template, and the associated Door Template, the setting in the Wiring Template takes precedence.

A preconfigured wiring template for each of the following subpanels is provided:

- MR50
- MR51e
- MR52
- MR62e
- 1501 Internal SIO
- 1502 Internal SIO

You can modify the preconfigured wiring templates and create new wiring templates for each type of subpanel in use at your site. If you use different wiring setups for the same type of subpanel, create a wiring template for each setup.

**Important:** Before you configure the wiring template for a subpanel, you should have already configured the reader templates, input templates, and output templates needed for that subpanel. A

wiring template contains mappings for the subpanel input, output, and reader addresses that correspond to the wiring set up of the subpanel for the readers, door position, strike, and request to exit (REX) buttons, and sets the associated template for each mapping. The number of doors and available reader, input, and output addresses for mapping is fixed for each subpanel model.

To access wiring templates, select **Physical Access** > **Templates** and then click the **Wiring Templates** tab. The **Wiring Templates** list page is displayed. This page lists all wiring templates that have been defined in the system.

## Wiring Templates list page

When you select **Physical Access** > **Templates** and click the **Wiring Templates** tab, the Wiring Templates list page is displayed. This page lists all wiring templates that have been defined in the system.

| Feature | Description |
|---|---|
| **Name** | The name of the wiring template.<br>Click the name to edit the wiring template details. |
| **Delete** | Click to delete the wiring template. |
| | Click to add a new wiring template. |

## Wiring Template: Add page

When you click on the **Wiring Templates** list page, the **Wiring Template: Add** page appears. Enter the wiring template details.

You can check if the settings you make on this page are valid at any time by clicking **Validate** at the bottom of the page. If there is an error on the page, an error message identifies the problem for you to correct.

| Feature | Description |
|---|---|
| **Name** | Enter a unique name for the template. |
| **Vendor** | The only option is **Mercury Security**. |

| Feature | Description |
|---|---|
| **Model** | Select from the drop-down list: |

**Subpanels for Doors and Readers**

| Model | Number of Doors | Number of Readers |
|---|---|---|
| **MR50** | 1 | 2 |
| **MR52** | 2 | 4 |
| **1502 Internal SIO** | 2 | 4 |
| **MR51e** | 2 | 4 |
| **MR62e** | 2 | 4 |
| **1501 Internal SIO** | 2 | 4 |
| **M5-2RP** | 2 | 2 |
| **M5-2SRP** | 2 | 2 |
| **M5-8RP** | 8 | 8 |
| **MS-2K** | 4 | 4 |
| **MS-ACS** | 8 | 8 |
| **4502 Internal SIO** | 2 | 4 |

or

**Subpanels for Inputs or Outputs (I/O)**

| Model |
|---|
| **MR161N** |
| **MR16OUT** |
| **M5-20IN** |
| **M5-16DO** |
| **M5-16DOR** |
| **M8-I8S** |
| **M8-R8S** |

**For each door:**

| Feature | Description |
|---|---|
| **Door** | Select an **Access Type** from the drop-down list:<br>• **Single**: A door connected to a single reader using any supported connection protocol on a single port.<br>• **Paired**: A door connected to two readers on the same port. A second pair of template settings is displayed.<br>For the single door or both paired doors select:<br>• **Door Template**<br>• **Reader**: Address and Reader Template<br>• **Alt Reader**: Address and Reader Template<br>**Important:** When using OSDP readers, you need four OSDP reader templates for a paired door: one for each OSDP address.<br>Specify the I/O templates for the doors created with this template:<br>Door Position Address: Input Template<br>Strike: Output Template<br>REX 1: Input Template<br>REX 2: Input Template |
| **For Other I/O** | |
| | Select an **Input Template** to use for all inputs not associated with doors. |
| | Select an **Output Template** to use for all outputs not associated with doors. |
| **Save** | Click to save the template and return to the Wiring Templates list page. |
| **Cancel Changes** | Click to return to the Wiring Templates list page without saving. |
| **Add Wiring Template** | Click to add a new wiring template. |

### Wiring Template: Edit page

When you click on the name of a template on the Wiring Templates list page, the Wiring Template: Edit page is displayed. Use this page to modify the wiring template.

You can check if the settings you make on this page are valid at any time by clicking **Validate** at the bottom of the page. If there is an error on the page, an error message identifies the problem for you to correct.

For details about the fields on this page, see *Wiring Template: Add page* on page 153

# Configuring Panels

Panels are controllers that connect one or more door controllers (subpanels) and their associated readers to the ACM appliance. Through an Ethernet cable or encrypted wireless connection, panels send information

about the state of the doors back to the appliance. Panels are added one at a time.

When a new Mercury panel is created you can use the Subpanel: Batch Create wizard to add subpanels to the panel. The wizard adds connection information for the subpanels and doors that are wired to the panel so that the ACM appliance can start managing door access. You must configure door templates, input templates, output templates, reader templates, and wiring templates before you can use the wizard. Together, these templates can provide enough information to ensure basic functioning of doors as soon as the new panel and subpanels are fully connected and communicating with the ACM system. For more information, see *Templates Overview* on page 133.

**Tip:** To add a gateway to manage Schlage IP wireless locks, see *Step 2: Configuring Gateways for IP-enabled Wireless Locks* on page 268. To add a SALTO server and panel to manage SALTO doors, see *Step 1: Connecting to a SALTO Server* on page 285. To add a Door Server Router (DSR) panel to manage ASSA ABLOY IP-enabled locks, see *Step 1: Configuring a Door Service Router for IP-enabled Locks* on page 295.

## Searching for Panels

Many facilities require the control and monitoring of dozens, even hundreds, of panels simultaneously. This can result in a crowded listing page. You can search for specific panels to narrow the list of panels appearing on the Panels list page.

1. Use any (or all) of the following to define your search:
    - Enter your search term in the **Search...** field. Use any series of letters and numbers to search for the panels you want to see.
    - If known, select the **Device Status**.
    - If known, select the **Appliance** the panel is connected to.
    - If known, select the **Group** the panel is included in.
2. Click **OK**.

## Panel Migration

Migrate panel models without reprogramming their settings and reduce system downtime.

### HID VertX V1000 to Mercury Security LP4502

**Note:** This procedure requires Mercury firmware version 1.30.5.

**CAUTION —** Upgrading from a V1000 to LP4502 panel model is irreversible. Perform this configuration only if needed. Before you start the migration, the V1000 panel must be uninstalled.

**Note:** After migration, all HID subpanels, doors, inputs, outputs and schedules will be maintained. Any HID V100 doors connected to V1000 panels will be displayed as Mercury Security doors. All HID

V100 door attributes will be retained with the following exceptions:

- APB Mode field on the Door: Edit Operations tab
  - Hard Door APB will be migrated to Door-Based Timed APB.

    Any time limit in the APB Delay field will be retained. If there is no time limit in the APB Delay field before the migration, the door no longer generates an APB error and instead generates a Local Grant event, when the card is swiped.
  - Soft Door APB is no longer displayed. Each badge can still access the door, however, the door no longer generates a Local Grant - APB Error - Used event when the card is swiped.
- Door use Tracking door processing attribute and Offline Door Mode are no longer supported on the Door Edit: Parameters tab.

To upgrade a V1000 panel to an LP4502 panel:

1. Uninstall the V1000 panel in the ACM application.
   a. Go to the **Host** tab of the V1000 panel.
   b. Uncheck the **Installed** checkbox.
   c. Click .
2. Install the LP4502 panel in the ACM application.
   a. Go to the **Configure** tab of the V1000 panel.
   b. Select **Mercury Security** instead of **HID** in **Vendor**.
   c. Select **LP4502** in **Model**.
   d. Click and then **OK** to continue.
   e. Click . Allow a few minutes for the update to complete.
3. Disconnect the V1000 wires and connect them to the ports on the LP4502 panel.
   - Connect port 1 and 2 on the V1000 panel to port 1 on the LP4502 panel.
   - Connect port 3 and 4 on the V1000 panel to port 2 on the LP4502 panel.

   **Note:** Each LP4502 port supports only one protocol. Make sure the protocol used by the HID subpanels match the protocol used by the LP4502 panel. In addition, make sure the location has adequate physical power for the LP4502 panel model.
4. Connect to the LP4502 panel on the **Host** tab of the Mercury Security panel:
   a. Enter the IP address of the LP4502 panel in **IP Address**.
   b. Click the **Installed** checkbox to enter a checkmark.
   c. Click . The tokens are downloaded to the panel automatically.

> **Note:** The subpanel port (default) assignment is updated on the Status tab:
>
> - V1000 subpanels on ports 1 and 2 are mapped to port 1 on the LP4502 panel.
> - V1000 subpanels on ports 3 and 4 are mapped to port 2 on the LP4502 panel.

5. Reset the panel after changing the panel model.

   For more information, see *Resetting Doors Connected to a Subpanel* on page 170.
6. Test the mapped port connections.
   a. On the **Status** tab of the V1000 panel, click the port 1 or port 2 link in the lower-right **Subpanel** list.
   b. On the **Status** tab of the subpanel, make sure color-based status changes occur for any of the following actions:
      - Click the **On** button to activate an output.
      - Click the **Off** button to deactivate an output.

### Mercury Security EP to LP Panel

**CAUTION —** Upgrading from an EP to LP panel model is irreversible. Perform this configuration only if needed. Before migrating a model 'with downstream' to a model 'without downstream,' ensure all wired subpanels are removed.

To upgrade an EP panel to an LP panel:

1. On the **Configure** tab of the EP panel:
   a. Select the applicable LP model in **Model**.

      For EP1501 and LP1501 models, converting between 'with downstream' and 'without downstream' options is supported.
   b. Click .
2. Reset the panel after changing the panel model.

   For more information, see *Resetting Doors Connected to a Subpanel* on page 170.

## Adding Panels

Panels connect door controllers and their readers to the ACM appliance. Adding a panel to the ACM system allows the appliance to gather information on the connected doors.

> **Tip:** To add a gateway to manage Schlage IP wireless locks, see *Step 2: Configuring Gateways for IP-enabled Wireless Locks* on page 268. To add a SALTO server and panel to manage SALTO doors, see *Step 1: Connecting to a SALTO Server* on page 285. To add a Door Server Router (DSR) panel to manage ASSA ABLOY IP-enabled locks, see *Step 1: Configuring a Door Service Router for IP-enabled Locks* on page 295.

To add a panel to the system:

1. Select **Physical Access>Panels**.

2. Click **Add Panel**.
3. Enter:

| | |
|---|---|
| **Name** | A unique name for the panel. Choose a name that will help you identify the devices it controls. Duplicate names are not allowed. |
| **Physical Location** | A description of where the device is installed. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Appliance** | The ACM appliance that is connected to the panel. |
| **Vendor** | The vendor of the panel or gateway. |
| | If **HID** is selected, enter:<br>**Model**: The V1000 or V2000 model of the panel.<br>**Timezone**: The local time which the panel operates in for door schedules and other time-based configuration. |

If **Mercury Security** is selected, enter:

**Model**: The model of the Mercury panel.

> **Tip:** Lenel panels can be configured as Mercury panels. For more information, see *Lenel Panel Support* on page 169.

**Enable Large Encoded Card Format**: For all types of Mercury controllers other than the LP4502 model with the pivCLASS with external PAM. See *Appendix: pivCLASS Configuration* on page 503.

**Embedded Auth**: For LP4502 model only. See *Appendix: pivCLASS Configuration* on page 503.

**Timezone**: The local time which the panel operates in for door schedules and other time-based configuration.

**Wiring Type**: For SCP models only. The type of port the panel uses to connect to door or subpanels.

For SCP-2 and SCP-E models, enter:

- **(4) 2-Wire Ports**
- **(2) 4-Wire Ports**
- **(1) 4-Wire/(2) 2-Wire**

For SCP-C model, enter:

- **(2) 2-Wire Ports**
- **(1) 4-Wire Port**

**Total Memory**: For SCP-2 and SCP-E models only. The total memory the panel contains.

**Max Elevator Floors**: For SCP models only. The number of floors the panel oversees. Up to 128 floors can be specified. For more information on defining elevator door access, see *Managing Elevator Access* on page 124.

**Allocate space :**

**Credentials**: The number of credentials that can be stored in the panel. The number is dependent on the memory, vendor and model of the panel.

**Events**: The number of transactions to buffer in the panel. The number is dependent on the memory, vendor and model of the panel.

**Version**: The current version of the database.

---

If **Schlage** is selected, enter:

**Site** : The name of the site that the gateway is commissioned to.

**Model**: **ENGAGE Gateway - IP**

---

**Installed** — If selected, the panel is installed and ready to communicate with the ACM appliance.

4. Click ✔ to save your changes.

   Click ✖ to discard your changes.

After you add a new panel for:

- HID V1000 model, see *Subpanel: Batch Add page (VertX®)* on page 166
- HID V2000 model, see *Subpanel Fields* on page 165
- Any Mercury Security model, see *Batch Creating Subpanels on a New Mercury Panel* below. However, see *Adding a Subpanel* on page 173 if the panel is wired to an AD-300 or PIM400 model subpanel , or the LP4502 panel is wired to an HID VertX V100, V200, or V300 subpanel.

After you add a new gateway for:

- Schlage ENGAGE Gateway for Schlage RSI wireless locks, see *Adding a Subpanel* on page 173
- Schlage ENGAGE Gateway for Schlage IP wireless locks, see *Step 3: Configuring IP-enabled Wireless Devices* on page 269

See also:

- *Deleting Doors* on page 202

## Configuring the Mercury Security MS Bridge Solution

To use the Mercury Security MS Bridge controllers and subpanels, you must have at least the following connected to the system:

- Mercury MS-ICS panel with downstream support.
- Mercury MS-ACS subpanel that is wired to the Mercury panel.

1. Add a Mercury MS-ICS panel to the ACM system.

   For more information, see *Adding Panels* on page 158.
2. Use the Batch Create wizard to add all required subpanels (the maximum number of subpanels is 32) to the new panel.

   For more information, see *Adding Mercury Security Panels* on page 164.

   **Note:** Add at least one MS-ACS (maximum two) as a subpanel.

   **Note:** You can add any Mercury panels that use the same protocol.
3. After all subpanels have been added to the system, select the **Subpanels** tab and click in the **Installed** column of the displayed table for each subpanel so that a ✔ displays.
4. Create the related doors. Ensure that for each door you select the corresponding Mercury panel and subpanel.

   For more information, see *Adding Doors* on page 214.
5. Customize the door settings to meet your system requirements and save your changes.

## Batch Creating Subpanels on a New Mercury Panel

Does not apply to:

- LP4502 panels that are wired to HID VertX V100, V200, and V300 subpanels
- Schlage AD-300 and PIM-400 subpanels, Aperio and SmartIntego subpanels, and RSI ENGAGE gateways

Mercury internal subpanels on the EP1501, LP1501, EP1502, LP1502 and LP4502 models do not have an address that can be changed.

After you save a new Mercury panel, you are prompted to use the Subpanel: Batch Create wizard. The wizard lets you create identically configured doors on many types of subpanels, as well as groups of doors configured differently on the same type of subpanel, and to name all the doors all in a single session.

The wizard lets you quickly create many subpanels and doors at once. The optional wiring templates allow you to give your subpanels standard configurations for inputs, outputs and doors. Doors will only be created when they are defined in the selected wiring templates. These templates must be configured before the wizard can use them to create functioning subpanels and doors. The more you standardize doors, readers, outputs, inputs, and panel wiring, the fewer templates you need. Some sample templates are provided. For more information, see *Templates Overview* on page 133.

The wizard is only available when you create a new Mercury panel. Its use is optional. You can cancel out of the wizard and the panel is still saved. However, you will have to configure all of your subpanels and the doors, readers, outputs, and inputs to each subpanel individually.

**Important:** To bulk add door subpanels when adding a new Mercury panel, you must use a door template that has a value specified for Door Mode. Before using the Subpanel: Batch Create wizard, ensure that a door template for the door subpanel type has been configured. Door templates without a Door Mode specified are not available for the wizard to use.

In the wizard, entering subpanel information is a three-step procedure:

1. Batch Create: Add a row for each type of subpanel that uses the same wiring template. In each row, identify the subpanel type, the base name shared by all subpanels, the number of subpanels, and the wiring template to use. You can only add as many subpanels as the panel can support. You can only select a wiring template that supports that subpanel type. You can use the wizard to create unpopulated subpanels by not specifying a wiring template.
2. Batch Edit: A row is displayed for each subpanel to be created. All the values can be changed. If you change the subpanel type, you also have to change the wiring template. You can also add more subpanels, up to the maximum supported by the panel.
3. Batch Name Doors: Edit the default door names for any door to conform to your site's standard method for identifying doors (such as room numbers or names).

   or

   Batch Create Summary: If no doors are configured for the subpanel, review the details.

Each step is completed on its own page. Checks are made as you enter data to ensure that you enter only valid data for the panel and subpanels, and do not overpopulate the panel. The subpanels are created when you click **Save** after completing the third step.

You can move between these three pages using **Next** and **Previous** buttons. If you press **Previous**, the `Going back will erase all progress from this page, are you sure?` message is displayed and you have to choose to proceed. You can click **Cancel Changes** in any step to exit the wizard without creating any subpanels, although the panel has already been created.

**Tip:** After you have configured new doors using templates, you must access each door, panel, or subpanel to configure the unique settings that are not configured by each template.

***Subpanel: Batch Create page***

| | |
|---|---|
| To add a subpanel: | Click + |
| To remove a subpanel: | Click − |

Add a row for each differently configured subpanel connected to the new panel, up to the maximum supported for that type of panel. Typically, this would be one row for each type of subpanel. In each row, specify the type of subpanel, its base name, the number of subpanels to create, and the templates to use to create them.

> **Note:** An exception to this is the MS-ISC panel, which only supports two MS-ACS subpanels, with addresses 0 and 2. You can add more than two MS-ACS subpanels to an MS-ISC panel on the first page, but you must correct this on the Subpanel: Batch Edit Details page before you can proceed to the Subpanel: Batch Name Doors.

Most controllers have a built-in subpanel. That subpanel will be automatically created as part of the batch add process. You cannot delete it or change its type, name, quantity or address.

| Column | Description |
|---|---|
| **Subpanel Type** | Select the subpanel model from the Select Model drop-down list. The selection is determined by the panel model. |
| **Subpanel Base Name** | The prefix used in the name of each subpanel. The default format is <panelName>-<panelModel>. For example EastEntrance-LP2500. You can change this name. |
| **Quantity** | Select the number of identically configured subpanels you want to add. The number of available subpanels is updated as new rows are added. |
| **Wiring Template** | Select the template from the Select Wiring Template drop-down list. The selection is determined by the subpanel type.<br><br>**Important for users of templates created in releases prior to ACM Release 6.0**: If you select a template that supports doors that has no doors associated with it, the `Selected template has no door profiles` warning message is displayed. This warning usually occurs for wiring templates created prior to ACM Release 6.0 that have not been modified to associate them with doors. You can choose to continue (and no doors will be created by the wizard) or edit the template. To edit the template, click the **Edit Template** button that is now displayed . |

Click **Next** and the **Subpanel: Batch Edit Details** page is displayed.

***Subpanel: Batch Edit Details page***

| | |
|---|---|
| To add a subpanel: | Click + |
| To remove a subpanel: | Click − |

Edit the details for all of the subpanels you added for the new panel. You can also continue to add and remove subpanels up to the maximum supported by the panel.

| Column | Description |
|---|---|
| **Address** | The port address on the panel to which the subpanel is connected. If there are addresses available, you can add and reorder the addresses. New subpanels are always added to the first available address.<br><br>**Note:** The MS-ISC panel only supports two MS-ACS subpanels, with addresses two 0 and 2. If you added more than two MS-ACS subpanels to an MS-ISC panel on the first page, you must correct this here before you can proceed to the Subpanel: Batch Name Doors. |
| **Subpanel Type** | You can change the subpanel type. After you make your selection, the row is updated to prompt you for the information needed to create the subpanel. |
| **Subpanel Name** | The name of each subpanel. The default name is the subpanel address appended to the Subpanel Base Name: <panelName>-<panelModel>-<subpanelAddress>. For example EastEntrance-LP2500-0. You can change this name. |
| **Wiring Template** | Select the template from the Select Wiring Template drop-down list. The selection is determined by the subpanel type. |

Click **Next**.

***Subpanel: Batch Name Doors or Subpanel: Batch Create Summary page***

If there are any doors to configure (because wiring templates with door configurations were selected), they can be named on the Subpanel: Batch Name Doors page that is displayed. Otherwise the Subpanel: Batch Create Summary page is presented. On both pages the settings you have configured on the previous pages are displayed for your review before the subpanels are created.

On the Subpanel: Batch Name Doors, default names for each door are displayed for each door subpanel being added to the panel. You can edit the door names to match the door-naming standard for your site before the subpanels are created.

Click **Save** to create the subpanels and doors and return to the **Panel: Edit** page. To access the subpanels you created, click the **Subpanels** tab.

## Adding HID VertX® Subpanels

If you selected VertX® as the panel vendor in the Panel Add page, complete the following procedure:

1. After you save the new panel, the Subpanel: Batch Add page is displayed.
2. Select the number of each subpanel model that is installed at each port then click .
   The HID Panel Configure page is displayed.
3. Select the **Host** tab.
4. Enter the IP address for this panel.
5. Click to save your changes.

## Adding Mercury Security Panels

If you selected Mercury Security as the panel vendor in the Panel Add page, complete the following

procedure:

1. After you save the new panel, the Subpanels: Batch Create  page is displayed.

   **Note:** The listed subpanel models will be different depending on the Mercury panel model that was selected on initial Panel Add page.

2. Select the number of subpanel models that are installed.
3. Click **Save**.
   The Mercury Security Panel Edit page is displayed.
4. Select the **Host** tab.
5. Enter the IP address for this panel.
6. Click to save your changes.

## Subpanel Fields

For Mercury Security, HID VertX, Schlage ENGAGE gateway (RSI mode) and ASSA ABLOY doors.

Add or edit a subpanel that is supported by the panel on the **Subpanels** tab in **Physical Access** > **Panels**.

**Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| | |
|---|---|
| **Name** | A name for the new subpanel, gateway or hub. |
| **Physical Location** | A brief description of where the subpanel, gateway or hub is located. |
| **Model** | The model of the new subpanel, gateway or hub. |
| **Port** | The port that the subpanel is connected to on the main panel.<br>For a Schlage AD-300 subpanel, the default is Port 2. For a SmartIntego GatewayNode, or ASSA ABLOY Aperio hub subpanel, the default is Network.<br>For an HID VertX V100, V200 or V300 subpanel, the default is RS485-1. |
| **Installed** | If checked, the subpanel is installed and able to communicate with the main panel. |
| **Address** | The RS-485 RSI or IP address for the selected port and for all subpanels except those that use the network port.<br>For a SimonsVoss GatewayNode subpanel, the hexadecimal address assigned by the SmartIntego Tool. |
| **Address Mode** | For the MR62e module only, DHCP or Static IP. |
| **Elevator Inputs** | For an MR16IN or MR52 subpanel if checked, the door module is used as an input for an elevator. |
| **Elevator Outputs** | For an MR16OUT or MR52 subpanel if checked, the door module is used as an output for an elevator. |
| **IP Address** | The subpanel IP address of a gateway or hub; or an MR51e subpanel or MR62e module operating in Static IP model. |

| | |
|---|---|
| **Hostname** | For an MR62e module, DHCP mode, the hostname of the panel.<br><br>The hostname of the gateway. |
| **MAC Address** | For an MR51e subpanel, the subpanel MAC address.<br><br>The MAC address of the gateway. |
| **Low Door** | For a Schlage RSI-based ENGAGE Gateway or PIM400 subpanel, the lowest door number in the series that is managed by the subpanel. The numbered doors managed by each subpanel cannot overlap. |
| **High Door** | For a Schlage RSI-based ENGAGE Gateway or PIM400 subpanel, the highest door number in the series that is managed by the subpanel. The numbered doors managed by each subpanel cannot overlap. |

### Subpanel: Batch Add page (VertX®)

This page appears if you are adding a new VertX® panel. After you save the initial panel details, this page allows you to batch add all the subpanels that may be connected to the controller panel.

| Feature | Description |
|---|---|
| **Port #** | The port on the panel that the subpanel is connected to. |
| **Model** | The supported subpanel models. |
| **Quantity** | Select the number of each subpanel that is installed at each port. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Editing Panels

To edit an existing panel, select the type of panels that you have installed.

### Editing HID® VertX® Panels

To edit an existing VertX® panel:

1. On the Panels  list, select the panel you want to edit.
   The HID Panel Status page is displayed.
2. If necessary, download configuration data, user data, or updated firmware to this panel.
3. Navigate the tabs on the screen to make the required changes.
   - **Configure** – select this tab to change the panel properties.
   - **Host** – select this tab to change the panel's network address.
   - **Subpanels** – select this tab to configure the subpanels that are connected to the panel.
   - **Events** – select this tab to review and configure the events that are associated with the panel.
4. Click  at the bottom of each page to save your changes.

### Editing Mercury Security Panels

To edit an existing Mercury Security panel:

1. On the Panels  list, select the panel you want to edit.

   The Mercury Security Panel Status page is displayed.
2. If necessary, download configuration data, user data, or updated firmware to this panel.
3. Select the any tabs on the screen to make the required changes.
   - **Configure** – select this tab to change the panel properties.
   - **Host** – select this tab to configure authentication of the panel, encryption of traffic to and from the panel, and to change the panel's network address.
   - **Subpanels** – select this tab to configure the subpanels that are connected to the panel.
   - **Macros** – select this tab to add or configure the macros used to perform system actions.
   - **Triggers** – select this tab to define what must occur before a macro is called into action.
   - **Access Levels** – select this tab to review the access levels that have been defined for the panel.
   - **Schedules** – select this tab to review the schedules that have been defined for the panel.
   - **Card Formats** – select this tab to view the card formats for all doors connected to the panel.
   - **Events** – select this tab to review and configure the events that are associated with the panel.
4. Click ✔ at the bottom of each page to save your changes.

## Panel Card Formats

When you click the **Card Formats** tab from the Panel: Edit page the Panel Card Formats page is displayed.

This read-only page displays a table that lists the card formats used on all the doors connected to that panel. Although the ACM system allows you to define up to 128 card formats system-wide, only 16 card formats can be used within a single panel.

You can use this table to identify the doors that use each card format. Each row displays a card format in the Card Formats column, and displays a drop-down menu that displays the number of doors that recognize this. Click on the drop-down menu bar to see the list of doors.

## ENGAGE Gateway Configuration

On the **Panel: Edit Configure** tab, see:

| | |
|---|---|
| **Name** | Up to 50 characters for the name of the gateway. |
| **Physical Location** | A description of where the device is installed. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Appliance** | The ACM appliance the device is connected to. |
| **Vendor** | Select **Schlage**.<br><br>**Model**: **ENGAGE Gateway - IP**.<br><br>**Site** : The name of the site that the gateway is commissioned to.<br><br>**Timeszone** : The local timezone where the gateway is installed. |

See also:

- *Step 2: Configuring Gateways for IP-enabled Wireless Locks* on page 268

## SALTO Panel Status

On the **Panel: Status** tab, see:

| | |
|---|---|
| | The communications status between the SALTO server and ACM appliance. The current status of the device is indicated by the background color. For more information, see *Status Colors* on page 43. |
| **Server Time/Date** | The date and time of the last import from the SALTO server to the ACM appliance. |
| **Language Code** | The language code used. |
| **Protocol Version** | The SALTO Host Interface Protocol version. |
| **Notes** | Add notes about the panel and review previous notes, if any. |

See also:

- *Step 3: Syncing Doors with the SALTO Server* on page 286
- *Downloading All Tokens* on page 292

## SALTO Panel Configuration

On the **Panel: Edit Configure** tab, see:

| | |
|---|---|
| **Name** | Read-only. Up to 50 characters for the name of the server. |
| **Physical Location** | A description of where the device is installed. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Appliance** | Read-only. The ACM appliance the device is connected to. |
| **Vendor** | Read-only. **SALTO**. |
| **Installed** | Enables communication between the ACM appliance and server after saving. |

See also:

- *Step 2: Configuring the SALTO Server* on page 286

## ASSA ABLOY Panel Configuration

On the **Panel: Edit Configure** tab, see:

| | |
|---|---|
| **Name** | Read-only. Up to 50 characters for the name of the server. |
| **Physical Location** | A description of where the device is installed. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Appliance** | Read-only. The ACM appliance the device is connected to. |
| **Vendor** | Read-only. **ASSA ABLOY**. |
| **Installed** | Enables communication between the ACM appliance and server after saving. |

See also:

- *Step 1: Configuring a Door Service Router for IP-enabled Locks* on page 295

## Resetting Anti-Passback from the Panel

In the event of an emergency, all the people in a building may leave an area at once and arrive at a mustering area together without using their access card at each door they encounter. This may cause the system to detect multiple anti-passback conditions.

To avoid granting each individual a free pass, you can reset the anti-passback condition for the panel.

1. On the Panels  list, select the panel you want to update.
2. On the Panel Status page, click **APB Reset**.

A confirmation message is displayed when APB is reset. Badge holders can return to their regular stations and the system will resume normal operations.

## Downloading Parameters

Any changes you make to the panel configuration or related events are automatically downloaded to the panel daily. However, you can manually download the parameters to immediately activate the updated configurations.

1. On the Panels  list, select the panel you want to update.
2. On the Panel Status page, click **Parameters**.

The application downloads the configured parameters to the panel.

## Downloading Tokens

Whenever you add new identities or update door access information in the system, the system automatically downloads the new details to the panels and doors. However, if the auto-download is unsuccessful, you can download tokens to the panel manually.

1. On the Panels  list, select the panel you want to update.
2. On the Panel Status page, click **Tokens**.

The tokens are downloaded to the panel.

## Lenel Panel Support

ACM appliances support Lenel panels but you must configure the Lenel panels as Mercury Security panels in the system.

The following table shows the equivalent Mercury Security panel for each supported Lenel panel.

| Mercury Security Panel Model | Lenel Panel Model |
|---|---|
| **SCP-C** | LNL-500 |
| **SCP-2** | LNL-1000 |
| **SCP-E** | LNL-2000 |
| **EP1502** | LNL-2220 |
| **EP2500** | LNL-3300 |
| **EP1501** | LNL-2210 |
| **MR16in** | LNL-1100 |
| **MR16out** | LNL-1200 |
| **MR50** | LNL-1300 |

| Mercury Security Panel Model | Lenel Panel Model |
|---|---|
| **MR52** | LNL-1320 |

For example, you have installed a Lenel **LNL-1000** panel. As you complete the procedure to add the new panel, you would select **Mercury Security** as the vendor and select the **SCP-2** as the model.

Since the SCP-2 and the LNL-1000 use the same parameters, the ACM appliance can communicate with the panels in the same way.

## Resetting Doors Connected to a Subpanel

All the subpanels that are connected to the panel can be reset with the latest configurations downloaded from the ACM system. The download includes any tokens, macros, triggers, inputs, outputs, and reader configurations.

To reset all the doors that are connected to a specific panel:

1. Click **Physical Access** > **Panels**.
2. Click the panel you want to reset.
3. Click the **Reset/Download** button on the Panel: Status page.

> **Note:** Allow several minutes for the download to complete.

Doors connected to the panel are now updated with the most recent configuration.

## Updating Panel Firmware

You can upload firmware updates to the panel, activate the new firmware and apply the latest ACM system configuration parameters.

> **CAUTION —** Risk of loss of functionality. It is possible to downgrade to an earlier firmware version by choosing an earlier firmware file. If you do downgrade to an earlier firmware release, functionality provided in later releases will no longer be available, resulting in unexpected behavior. For example, override functionality available for Mercury panels in the ACM software 5.12.2 and later, requires the Mercury firmware version 1.27.1 or later.

1. On the Panels list, select the panel.
2. On the Panel: Status page, click **Firmware**.

   > **Note:** For IP wireless locks, a firmware update is applied to all locks of the same type managed by the gateway (for example, NDE locks but not LE locks). For offline Wi-Fi locks, a firmware update is applied to the single selected lock.

3. Do any of the following:

- Apply a firmware update that is available in the system, click next to the firmware file.
- Upload a new firmware update provided by the manufacturer:
  a. Download the firmware file from the manufacturer.
  b. Click **Add Firmware**.

     See *Appendix: pivCLASS Configuration* on page 503.

  c. Click **Choose File** and select the firmware file.
  d. Click to upload the firmware file.

     > **Note:** If you click , the **Identity Import Type:** will be set to **Auto** and any attached CSV files will be deleted.

  e. On the Firmware list, click next to the firmware file to apply it to the panel.
- Delete an existing firmware update, click next to the firmware file. Click **OK** to confirm the operation.

## Updating Schlage Gateway Firmware

> **Note:** Ensure the ENGAGE gateway and ACM have access to the internet.

To apply gateway firmware updates:

1. On the Panels list, select the panel.
2. On the Panel: Status page, click **Firmware**.

   > **Note:** For IP wireless locks, a firmware update is applied to all locks of the same type managed by the gateway (for example, NDE locks but not LE locks). For offline Wi-Fi locks, a firmware update is applied to the single selected lock.

3. Do one of the following:
   - Click next to the firmware version that is available in the system to apply it to the group of locks.
   - Select a new firmware version as follows:
     a. Click **Open Advanced Options**.
     b. Enter your ENGAGE login information in **ENGAGE User** and **ENGAGE Password**, and click **Get Available Firmware**. The firmware versions are downloaded.

        **CAUTION —** This advanced procedure must be performed only by qualified personnel with the requisite knowledge of the firmware versions and the ACM system.

     c. Click next to the firmware file to apply it.

**Note:** For offline Wi-Fi locks, the firmware version update does not occur immediately. It occurs at the next communication interval to the ACM application. Each offline Wi-Fi lock has its own interval setting which is dependent on the timing of its initial communication with the ACM system.

## Updating Panel Time

Each panel tells time by synchronizing with a time server that is accessible on the network. For example, a network time protocol (NTP) server may be used. In the event of unexpected power or network failure, the panel may run independently for a while and need to be re-synchronized when everything is back online.

1. On the Panels  list, select the panel.
2. On the Panel: Status page, click **Clock**. The button is not displayed if clock synchronization is not supported.

The panel connects and synchronizes with the time server.

## Deleting Panels

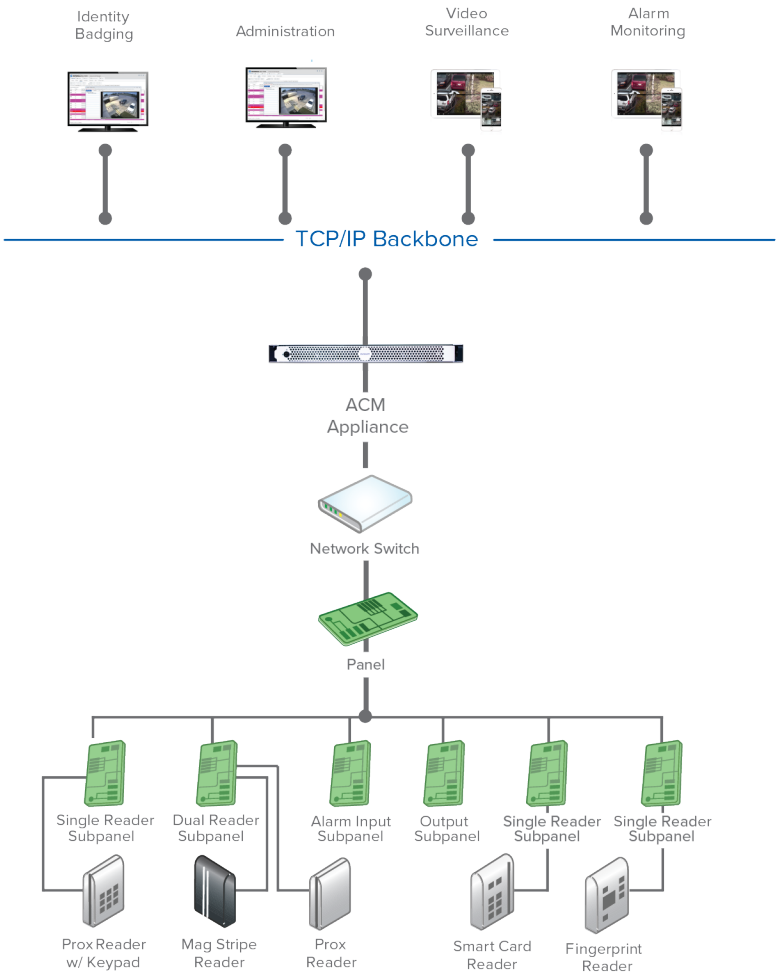
Deleting a panel removes the connection between the ACM system and the panel.

To delete the panel:

1. Select **Monitor** > **Dashboard** > **Panels** or **Physical Access** > **Panels**.
2. Click ... at the end of a row in the Panels table and then click **Delete**.
3. When the confirmation message appears, click **OK**.

## Configuring Subpanels

Some panels support hierarchical connections. One panel can be connected to a large number of specialized subpanels, and the subpanels transmit their data to the ACM appliance through the panel.




## Adding a Subpanel

Single subpanels can be added to a predefined panel. Gateway and hub subpanels can be added for wired and wireless locks.

> **Note:** HID VertX V100, V200, and V300 subpanels; Schlage PIM400, RSI-based ENGAGE Gateway, AD300; Assa Abloy Aperio; and SmartIntego GatewayNode subpanels can only be added one at a time to a Mercury panel. To batch add other supported subpanels, see *Batch Creating Subpanels on a New Mercury Panel* on page 161.

To add subpanels one at a time:

1. Select **Physical Access** > **Panels**.
2. Click the name of the panel that is wired to the new subpanel.
3. Select the **Subpanels** tab.
4. Click **Add Subpanel**.

5. Enter:

> **Note:** Fields in this list that are not supported by the subpanel or gateway are not displayed.

| | |
|---|---|
| **Name** | A name for the new subpanel, gateway or hub. |
| **Physical Location** | A brief description of where the subpanel, gateway or hub is located. |
| **Model** | The model of the new subpanel, gateway or hub. |
| **Port** | The port that the subpanel is connected to on the main panel.<br>For a Schlage AD-300 subpanel, the default is Port 2. For a SmartIntego GatewayNode, or ASSA ABLOY Aperio hub subpanel, the default is Network.<br>For an HID VertX V100, V200 or V300 subpanel, the default is RS485-1. |
| **Installed** | If checked, the subpanel is installed and able to communicate with the main panel. |
| **Address** | The RS-485 RSI or IP address for the selected port and for all subpanels except those that use the network port.<br>For a SimonsVoss GatewayNode subpanel, the hexadecimal address assigned by the SmartIntego Tool. |
| **Address Mode** | For the MR62e module only, DHCP or Static IP. |
| **Elevator Inputs** | For an MR16IN or MR52 subpanel if checked, the door module is used as an input for an elevator. |
| **Elevator Outputs** | For an MR16OUT or MR52 subpanel if checked, the door module is used as an output for an elevator. |
| **IP Address** | The subpanel IP address of a gateway or hub; or an MR51e subpanel or MR62e module operating in Static IP model. |
| **Hostname** | For an MR62e module, DHCP mode, the hostname of the panel.<br>The hostname of the gateway. |
| **MAC Address** | For an MR51e subpanel, the subpanel MAC address.<br>The MAC address of the gateway. |
| **Low Door** | For a Schlage RSI-based ENGAGE Gateway or PIM400 subpanel, the lowest door number in the series that is managed by the subpanel. The numbered doors managed by each subpanel cannot overlap. |
| **High Door** | For a Schlage RSI-based ENGAGE Gateway or PIM400 subpanel, the highest door number in the series that is managed by the subpanel. The numbered doors managed by each subpanel cannot overlap. |

6. Click to save your changes.

## Editing Subpanels

To edit an existing subpanel:

1. Select **Physical Access > Panels**.
2. Click the name of the panel the subpanel is connected to.
3. Select the **Subpanels** tab.
4. From the Subpanels list, perform any of the following:
    - To edit the subpanel details, click the subpanel name.
    - To edit the inputs connected to the subpanel, click for that subpanel.
    - To edit the outputs connected to the subpanel, click for that subpanel.
    - To edit the readers connected to the subpanel, click for that subpanel.
5. On the following listing page, select the specific device you want to edit.
6. Make the required changes to the device edit page.
7. Click to save your changes.

## Inputs

Inputs are associated with panels or doors and can include:

- Motion sensors
- Door contacts
- Smoke detectors
- REX (request to exit) buttons
- Perimeter and fence alarms
- Break glass window sensors
- Crash bars
- Capacitance duct sensors
- Device tamper switches

Inputs can be controlled in two ways:

- Masking
- Unmasking

Masked inputs do not trigger any corresponding outputs.

Unmasked inputs function normally.

The state may change according to several actions, including entry of a proper code or card, or operator override.

## Output Operating Modes

Outputs operate in **Operating Mode**. Operating mode describes how the output behaves during normal operation.

By choosing the Operating Mode option when editing an output, you can set one of the following options to define how the output behaves when it is active:

| Feature | Description |
|---|---|
| **Energized When Active** | An electrical current is expected to pass through the output point when it is active. |

| Feature | Description |
|---|---|
| **Not Energized When Active** | An electrical current is expected to pass through the output point when it is not active. |

### Outputs

Outputs are devices that perform tasks in response to input data. This includes unlocking a door, setting off a fire alarm, activating an elevator or turning off air conditioning. Output devices include:

- Strikes
- Magnetic locks
- Fire alarms
- Klaxons
- Motors of any sort
- HVAC

In general, these devices are activated by door controllers, panels, or subpanels that use relays to initiate activation. Output devices can have one of the following states:

- On (energized)
- Off (de-energized)
- Pulse (intermittently on and off)

Locks (in general) and strikes (specifically) come in several varieties that support a locked state that is either energized or de-energized, with a default state that is either locked or unlocked. This is for safety reasons. In the case of power outages and emergency shutdowns, many doors must 'fail open', meaning that they unlock whenever the power goes off, allowing people to exit an area. Other doors, such as bank vaults and secured areas, must 'fail close', meaning that a de-energized state requires the bolt to remain in place. For more on this, refer to *Configuring Doors* on page 189 and *Configuring Panels* on page 155.

Many outputs, such as sliding doors, alarms or warning lights need to be turned on *and* off. In order to do this, relays on many panels also provide a pulse feature that energizes the output for a specified amount of time then de-energizes the output for a specified amount of time.

Doors and other outputs can be activated by the user following a successful card or code entry. Alternatively, the operator can override normal operation or control the output on the Subpanel Status page.

### Deleting Subpanels

To disable communication between a panel and external subpanel, you can delete the subpanel from the system.

1. Select **Physical Access** > **Panels**.
2. Click the name of the panel that is connected to the external subpanel.
3. Select the **Subpanels** tab.
4. Click next to the subpanel name This button is not displayed for an internal subpanel.
5. When the confirmation message is displayed, click **OK**.

## Configuring Locks

To use locks with built-in card or PIN readers, add the related wireless lock subpanel to the system then add the lock hardware as part of a door. The readers can be either wired or wireless, depending on the lock.

## Supported Devices

After the locks with built-in card, PIN or fingerprint readers are installed and configured according to vendor instructions, ensure the physical configuration matches the configuration in the ACM application as follows. The readers can be either wired or wireless, depending on the lock.

> **Note:** To support the devices that connect to the LP series hubs, install the applicable LP_*nnnn*_1_30_0_662_FS_2_23.crc firmware versions. For more information about the firmware versions, see the ACM release notes.

| Door | Panel | | Subpanel | External System |
|---|---|---|---|---|
| **Wired locks** | | | | |
| *Allegion Schlage® AD-300 series* | | | | |
| Up to 8 wired locks to a panel port<br><br>Installed with a different number programmed into the locks for each set of doors to be connected to the panel. | Mercury Security EP1501, EP1501 with downstream communications support, EP2500, LP1501, LP1502, LP2500 or LP4502 | and | Up to 8 AD-300 subpanels.<br><br>Locks have built-in subpanels. | - |
| **Wireless locks** | | | | |
| *Allegion Schlage AD-400 series* | | | | |
| Up to 16 wireless locks<br><br>Each door communicates with the subpanel wirelessly. | Mercury Security EP2500, LP1501, LP1502, LP2500 or LP4502 | and | Up to 8 AD-400 subpanels to an RS-485 port on the controller.<br><br>Each subpanel is wired to a Mercury Security panel. | - |
| *Allegion Schlage LE and NDE series* | | | | |
| Up to 10 NDE and/or LE wireless locks operating in RSI mode to each gateway | Mercury Security EP2500, LP1502, LP2500 or LP4502 | or | Up to 8 NDE ENGAGE gateways to an RS-485 port on the controller.<br><br>Each subpanel is wired to a Mercury Security panel. | - |
| *ASSA ABLOY Aperio® series** | | | | |
| Up to 8 devices to an RS-485 hub<br><br>Each door communicates with the hub wirelessly. | Mercury Security EP1501, EP1501 with downstream support, EP1502, EP2500 or LP4502 | and | Aperio 1 to 8 Hub, or 1 to 1 Hub<br><br>See vendor documentation for the limit. | - |

| | | | | |
|---|---|---|---|---|
| Up to 64 devices to an IP hub<br><br>Door tamper is supported. | LP1502, LP2500 or LP4502 | and | Aperio AH40 IP Hub | - |
| *Aperio Wiegand devices and Wiegand hubs (1 device to 1 hub) are not managed in the ACM system. | | | | |
| *SimonsVoss series* | | | | |
| Up to 16 wireless locks to each gateway. | Mercury Security EP1501, EP1501 with downstream communications support, EP1502, EP2500 or MS-ICS panel | and | Up to 32 SmartIntego GatewayNode subpanels to a network port, depending on the panel.<br><br>Up to 16 gateways on Port 4 for EP1501.<br><br>Up to 32 gateways on Port 4 for EP1502, EP2500 and MS-ICS.<br><br>Each subpanel is connected over an Ethernet network using TCP. | - |

## Configuring ASSA ABLOY™ Aperio® Wireless Lock Technology

To use the ASSA ABLOY Aperio wireless locks, you must have the following panels connected to the system:

- Mercury Security EP1501, EP1501 with downstream support, EP1502, EP2500 or LP4502, or the LP series for the Aperio AH-40 Hub
- ASSA ABLOY Aperio 1 to 8 Hub, 1 to 1 Hub, or AH-40 Hub

**Note:** For the Aperio AH-40 Hub, ensure the **Enable TLS** checkbox is enabled on the hub's ACU settings in the Aperio programming application.

The wireless lock assembly is installed directly to the door and communicates with the Aperio Hub subpanel wirelessly.

1. Add the Mercury Security panel to the ACM system.

   For more information, see *Adding Panels* on page 158.
2. Add the **Aperio 1 to 8 Hub**, **Aperio 1 to 1 Hub**, or **Aperio AH-40 Hub**, as a subpanel to the panel added in the previous step.
   - For the Aperio AH-40 Hub subpanel, enter also the **IP Address**. For more information, see *Adding a Subpanel* on page 173.

     Enter also the **Aperio ACU Port** in the Appliance settings.

3. Add a door for each wireless lock assembly.
    a. For each door, select the corresponding Mercury Security panel, Aperio Hub subpanel and **Lock Number** that is assigned to the wireless lock assembly.
    b. For the Aperio AH-40 Hub subpanel, enter the **Device Id** (referred to as Lock/Sensor in the Aperio programming application).
    c. Customize all other door settings to meet your system requirements and save your changes.
    For more information, see *Adding Doors* on page 214.

## Configuring Allegion Schlage AD-400 Series Locks

To use Allegion Schlage AD-400 series locks, you must have the following panels connected to the system:

- Mercury Security EP1501, EP2500 with downstream support, or LP1502 panel
- Schalge PIM400 subpanel that is wired to the Mercury Security panel

The wireless lock assembly is installed directly to the door and communicates with the PIM400 subpanel wirelessly.

**Note:** Ensure the wireless locks are installed according to Schlage installation instructions.

1. Add a Mercury EP1501, EP2500 or LP1502 panel to the ACM system.

    For more information, see *Adding Panels* on page 158.
2. Add the PIM400 as a subpanel to the panel in the previous step.

    For more information, see *Adding Mercury Security Panels* on page 164.
3. After the panels have been added to the system, select the **Subpanels** tab.
4. For each PIM400 subpanel, enter the **Low Door** and **High Door** number that is assigned to the subpanel.

    Each PIM400 subpanel manages up to 16 wireless doors in a series. You must identify the lowest numbered door and the highest numbered door managed by each subpanel. The numbered doors managed by each subpanel cannot overlap.
5. Create a door for each wireless lock assembly.

    For more information, see *Adding Doors* on page 214.
6. For each door, select the corresponding Mercury Security panel, PIM400 subpanel and door number that is assigned to the wireless lock assembly.
7. On the door Parameters tab, you can set the **Lock Function** for the wireless locks. The options are:
    - **None**: Use the system default door settings.
    - **Privacy**: When the interior lock button is pressed, the door will lock and the exterior lock will not grant access to any token. To unlock the door, the interior lock button must be pressed again or exit the room.
    - **Apartment**: Use the interior lock button to toggle between locked and unlocked. When the door is locked, any valid token will open the door. The door must be manually locked or it will stay unlocked.
    - **Classroom — Classroom/Storeroom** — The lockset is normally secure. The inside lever always allows free egress. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may be used to change to a passage or secured status. Not to be used on mortise deadbolt. Interior push button not to be used.

> **Note:** This is the only lock function supported for the RSI-connected NDE series lock.

- **Office** — The lockset is normally secure. The inside lever always allows free egress. An interior push-button on the inside housing may be used to select a passage or secured status. Meets the need for lockdown function for safety and security. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may also be used to change status. Not to be used on mortise deadbolt.

> **Note:** A Restore door action is available on the Door listing page and the Hardware Status page which resets the Door Mode to its default value.

8. Customize all other door settings to meet your system requirements and save your changes.

## Configuring Allegion Schlage LE Series Locks

To use Allegion Schlage LE series locks, you must have one of the following panels connected to the system:

- Mercury Security EP1501, EP2500 with downstream support or LP1502 panel
- Schlage ENGAGE™ Gateway subpanel that is wired to the Mercury Security panel

> **Note:** Ensure the wireless locks are installed according to Schlage installation instructions.

1. Add a Mercury EP2500, EP1501 (with downstream) or LP1502 panel to the ACM system:
   a. Select **Physical Access>Panels**.
   b. Click ✚ .
   c. Enter the **Name**, **Vendor** and **Model**.
   d. Select **Installed**.
   e. Click ✔ to save.
2. Add the required subpanels to the new panel:
   - If using only ENGAGE Gateway subpanels, select the **Batch Add** option and click ✔ .

     > **Note:** Make sure the ENGAGE Gateway subpanel configuration matches the physical gateway.

   - If using both Gateway and non-Gateway subpanels, enter the correct number of Gateway subpanels and/or PIM400s on the Subpanel: Batch Add page (do not select any other panels at this stage) and click ✔ .

     For each ENGAGE Gateway subpanel:

a. Click the **Subpanels** tab. If you are adding non-Gateway subpanels, set the subpanels to the correct port.
b. Add the subpanel. You can mix and match any subpanels using the same Mercury Security protocol on the same port (such as ENGAGE Gateway and PIM400). For more information, see *Adding Mercury Security Panels* on page 164.
c. Select **Installed**.
d. Click to save.

3. Create a door for each wireless lock assembly.

   For more information, see *Adding Doors* on page 214.
4. For each door, select the corresponding Mercury Security panel, ENGAGE Gateway subpanel and door number that is assigned to the wireless lock assembly.
5. On the door Parameters tab, set the **Lock Function** for the wireless locks. The options are:
   - **None**: Use the system default door settings.
   - **Privacy**: When the interior lock button is pressed, the door will lock and the exterior lock will not grant access to any token. To unlock the door, the interior lock button must be pressed again or exit the room.
   - **Apartment**: Use the interior lock button to toggle between locked and unlocked. When the door is locked, any valid token will open the door. The door must be manually locked or it will stay unlocked.
   - **Classroom — Classroom/Storeroom** — The lockset is normally secure. The inside lever always allows free egress. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may be used to change to a passage or secured status. Not to be used on mortise deadbolt. Interior push button not to be used.

     **Note:** This is the only lock function supported for the RSI-connected NDE series lock.
   - **Office** — The lockset is normally secure. The inside lever always allows free egress. An interior push-button on the inside housing may be used to select a passage or secured status. Meets the need for lockdown function for safety and security. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may also be used to change status. Not to be used on mortise deadbolt.

   **Note:** A Restore door action is available on the Door listing page and the Hardware Status page which resets the Door Mode to its default value.
6. Customize all other door settings to meet your system requirements and save your changes.

## Configuring Allegion Schlage NDE Series Locks

To use Allegion Schlage NDE series locks, you must have one of the following panels connected to the system:

- Mercury EP1501 or EP2500 panel with downstream support.
- ENGAGE Gateway subpanel that is wired to the Mercury Security panel.

**Note:** Ensure that the wireless locks have been installed in line with Schlage's installation instructions.

1. Add a Mercury EP2500 or EP1501 (with downstream) panel to the ACM system:
   a. Select **Physical Access>Panels**.
   b. Click ✚ .
   c. Enter the **Name**, **Vendor** and **Model**.
   d. Select **Installed**.
   e. Click ✔ to save.
2. If you are adding:
   - just ENGAGE Gateway subpanels, then add all required subpanels to the panel created in the previous step using the Batch Add option and click ✔ .

     **Note:** You will still need to manually make sure that the ENGAGE Gateway has matching configuration as the physical gateway.
   - both Gateway and non-Gateway subpanels, then enter the correct number of Gateway subpanels and/or PIM400s on the Subpanel: Batch Add page (do not select any other panels at this stage) and click ✔ . For each other subpanel to be added:
     - Click on the **Subpanels** tab to open the Subpanel page. If you are adding non-Gateway subpanels ensure that the subpanels are set to the correct port.
     - Add the subpanel. You can mix and match any subpanels using the same Mercury Security protocol on the same port (i.e. ENGAGE Gateway and PIM400). For more information, see *Adding Mercury Security Panels* on page 164.

     For each ENGAGE Gateway subpanel, enter the following and select Installed:
     - **Port**
     - **Address**
     - **Low Door** and **High Door** number that is assigned to the subpanel.

     Each ENGAGE Gateway subpanel manages up to 10 NDE wireless doors. You must identify the lowest numbered door and the highest numbered door managed by each subpanel. The numbered doors managed by each subpanel cannot overlap.
3. Create a door for each wireless lock assembly.

   For more information, see *Adding Doors* on page 214.
4. For each door, select the corresponding Mercury Security panel, ENGAGE Gateway subpanel and door number that is assigned to the wireless lock assembly.
5. On the door Parameters tab, you can set the **Lock Function** for the wireless locks. For the NDE series there is only one lock function: **Classroom — Classroom/Storeroom**.

   **Note:** There is a Restore door action available on the Door listing page and the Hardware

Status page which resets the Door Mode to its default value.

6. Customize all other door settings to meet your system requirements and save your changes.

## Configuring SimonsVoss Wireless Locks

To use SimonsVoss series locks, you must have the following panels connected to the ACM system:

- Mercury EP1501 (with downstream support), EP1502, EP2500, or MS-ICS panel.
- SmartIntego GatewayNode subpanel that is connected over an Ethernet network using TCP. This connection is established after setting up the subpanel in the ACM software.

### *Prerequisites*

Ensure that the wireless locks have been installed and configured according to the SimonsVoss installation instructions. You must have:

- Configured the hostname, and optionally the IP address, or the MAC address in the SmartIntego GatewayNode software. For more information, refer to the SimonsVoss documentation for the SmartIntego GatewayNode software.

  **Note:** To use the MAC address of the wireless lock, the hostname must be configures in the format MAC<nnnnnnnnnnnn>, where nnnnnnnnnnnn is the MAC address without any colons. For example, the hostname for a lock with MAC address 12:34:56:78:9A:BC is entered MAC123456789ABC.

- Identified the hexadecimal address for each SmartIntego GatewayNode and each wireless lock before you can connect them to the ACM software. This information is available from the SmartIntego Tool as shown in the figures below. In these examples:
  - 0X0011 is the hex address for the SimonsVoss GatewayNode. Enter this value in the Address field for each SmartIntego GatewayNode in the ACM software (Physical Access > Panel > Subpanel).

    0X0016 is the hex address for the SimonsVoss wireless lock. This is the value entered in the Door Number field for each SImonsVoss lock in the ACM software (Physical Access > Doors > Add Door).

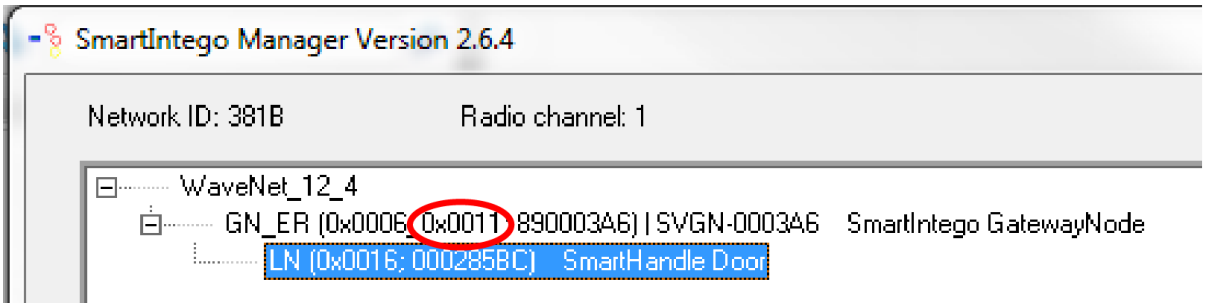



**Figure 2:** The SmartIntego GatewayNode hexadecimal address in the SmartIntego Manager screen of the SmartIntego Tool.

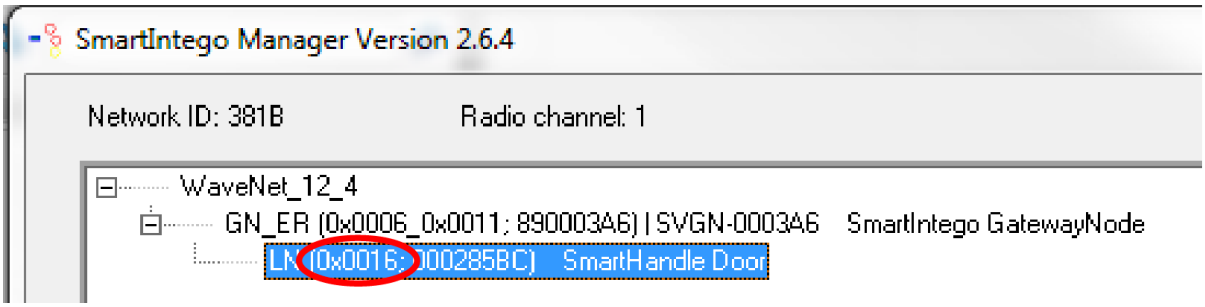



**Figure 3:** The SmartIntego lock hexadecimal address in the SmartIntego Manager screen of the SmartIntego Tool.

> **Note:** The SmartIntego Tool software and the SmartIntego GatewayNode software are not supported on Microsoft Windows 10.

***Configuring Doors***

To configure a door with a SmartIntego wireless lock in the ACM software, use the following steps:

1. Add a supported Mercury panel to the ACM system:
   a. Select **Physical Access>Panels**.
   b. Click ✚ .
   c. Enter the **Name**, **Vendor** and **Model**.
   d. Select **Installed**.
   e. Click ✔ to save.
2. Optionally, on the Subpanel: Batch Add panel, enter the number of SmartIntego GatewayNode subpanels. you want to add using the Batch Add option and click ✔ .
3. Click on the **Subpanels** tab to open the Subpanel page.
4. Open each SmartIntego GatewayNode subpanel and enter the following:
   - **Port**—Select Network and select **Installed**.
   - Enter at least one of the following
     - **IP Address**
     - **MAC Address**
     - **Hostname**
   - **Address**—enter the hexadecimal address for the SmartIntego GatewayNode.

   Each SmartIntego GatewayNode subpanel manages up to 16 wireless doors.

   > **Note:** You will still need to manually make sure that the subpanel configuration matches the physical gateway

5. Create a door for each wireless lock assembly. Ensure you specify Mercury Security as the vendor. For more information, see *Adding Doors* on page 214.

6. On the Parameters panel for each door, ensure that you do the following:
    - **Vendor** — Select Mercury Security
    - **Panel** — Select the panel that is connected to the SmartIntego GatewayNode for the door.
    - **Subpanel** — Select the subpanel for the SmartIntego GatewayNode that is connected to the door.
    - **Door Number** — Enter the hexadecimal address for the SmartIntego wireless lock assembly.
    - **Installed** — Click the checkbox.
    - **Don't pulse door strike on REX** — For SimonsVoss wireless locks, such as cylinders, that do not support a door position switch (DPOS) , this box must not be checked.
7. If the SimonsVoss lock on the door does not support a DPOS, the settings in the following fields have no effect:
    - On the parameters tab:
        - Mask Forced Schedule
        - Mask held Schedule
        - Always Mask Forced
        - Always Mask Held
        - Offline Mode
        - Deny Duress
        - Door Forced Filter
        - Enable cipher Mode
        - Use Shunt Relay
        - Detailed Events
        - do Not Log Rex Transactions
        - Log all grants right away
    - On the Operations tab:
        - APB Mode
        - APB Delay
        - Into Area
        - Out of Area
        - PIN Timeout
        - PIN Attempts
        - LED Mode
        - Held Open Time
        - Held Pre Alarm Access Time
        - Extended Access
        - Extended Held Open Time
        - Simple Macros
        - Strike Mode
        - Access time when open
        - Card Format
        - The Door status will default to Normal Status
8. Customize the other door settings to meet your system requirements and click .

The ACM system and the SmartIntego GatewayNode subpanel should now connect and the door should be

online.

***Troubleshooting***

### Door Is Not Online

If the door is not online:

- Wait a few minutes: The GatewayNode polls the SimonsVoss wireless lock three times in three minutes, then polls every three hours, until the door responds. Normally, the door should come online within three minutes.
- If the door is not online within a few minutes: Check all the connections between the ACM system and the SmartIntego GatewayNode subpanel, including the power.

### Door Status

After the door is operational, certain conditions of the SimonsVoss wireless lock that change the door status are not always immediately reported to the ACM system. As a result, the door status reported in the ACM client may not always accurately reflect the actual status of the of the door.

- If you uninstall the door and then reinstall it in the ACM system, the connection between the SmartIntego GatewayNode subpanel and the SimonsVoss lock is not interrupted. However, the reinstalled door will appear offline to the ACM system until the SmartIntego GatewayNode subpanel polls the SimonsVoss lock. This poll happens once every 12 hours, so you may have to wait as long as 12 hours. During this period, the door will function normally but the ACM system will not receive any events from the door.
- After a power outage to the SmartIntego GatewayNode subpanel, an accurate door status will not be seen in the ACM system until after the SmartIntego GatewayNode subpanel is online and polling of all the SimonsVoss doors connected to that subpanel has completed. The time it takes for the subpanel to come online and start polling can be variable.
- If the batteries in the SimonsVoss lock are depleted or removed, an accurate door status will not be seen in the ACM system until after 24 hours have elapsed since the last battery status report was received from the wireless lock. It could take up to 24 hours after battery power has been lost before the status is correctly reported. Meanwhile, commands can be sent to the door, but nothing happens.

**Note:** The ACM lockdown priority operation is superseded by the Escape and Return state of the SimonsVoss wireless lock when it becomes engaged in a lockdown situation.

## Macros

**Note:** Only Mercury Security panels support macros.

Macros are commands, or sequences of commands, that can control the activity of devices connected to a door, panel, or group of panels.

Macros can be extremely simple, such as turning out lights or masking an input. Or, they can be sophisticated multi-step procedures. For example, you can define a macro that closes down the air conditioning system, unmasks the alarms, locks all the doors connected to a panel, turns out the lights, then emails the operator for more instructions.

In the Avigilon ACM application, macros can be activated by:

- Triggers
- Interlocks

All doors (not limited to Mercury Security) support simple macros. Simple macros are triggered by a single door event and activate one output in response. For more information, see *Adding Simple Macros* on page 200.

## Adding Macros

1. Select **Physical Access** > **Panels**.
2. Click the name of the panel that you want to add a macro to.
3. On the Macros page, click **Add Macro**.

   Macros and macro commands are supported for triggers only. Macros and macro commands associated with interlocks are not supported (read-only).
4. On the following Macro Command  list, click the Macro link to change the macro name. In the new text field, enter a new name for the macro then click **OK**.
5. Click **Add Macro Command**.
6. Give the macro command a name.
7. From the **Command** drop down list, select a macro command.
8. If extra options are displayed after you select a macro command, choose the options you need.
9. From the Group drop down list, select the group you want to assign this macro to.
10. Click  to save your changes.
11. Back at the Macro Command page, repeat the previous steps until you've added all the commands that are required for this macro.

To apply this macro to a specific situation, see *Assigning Macros* on the next page.

To create quick macros that are specific to a particular door (simple macros), see *Adding Simple Macros* on page 200.

## Editing Macros

1. Select **Physical Access** > **Panels**.
2. Click the name of the panel with the macro you want to edit.
3. On the Macros page, click the name of the macro you want to edit.

   Macros and macro commands are supported for triggers only. Macros and macro commands associated with interlocks are not supported (read-only).
4. On the following Macro Command  list, perform any of the following:
   - To change the macro name, click the Macro name link. Enter a new name then click **OK**.
   - To add a new macro command, click **Add Macro Command**.
   - To edit a macro command, click the command type name.
   - To delete a macro command, click  for the command.
   - To change the order of the macro commands, click **Sort**.

## Deleting Macros

1. Select **Physical Access** > **Panels**.
2. Click the name of the panel with the macro you want to delete.
3. On the Macros page, click for the macro you want to delete.
4. When the confirmation message appears, click **OK**.

## Assigning Macros

> **Note:** Only Mercury Security doors and panels support macros.

Once you have created a macro, you can assign them to specific triggers or other macros so that they can automatically perform a series of actions under the right conditions.

### *Assigning a Macro to a Trigger*

When you add a trigger to a panel, assigning a macro is part of the process. Triggers and macros work together as a cause and effect pair. When the all the triggering conditions are met, the macro is automatically initiated.

To assign a macro to a trigger:

1. Add a macro. For more information, see *Adding Macros* on the previous page.
2. Add a trigger. For more information, see *Adding Triggers* on the next page.
3. In the Trigger Add page, assign the new macro to the trigger.
4. Click .

### *Assigning a Macro to a Macro*

You can activate a macro as part of a macro command to generate a complex series of actions.

To assign a macro to a macro command:

1. Add a macro. For more information, see *Adding Macros* on the previous page.
2. When you add a new macro command, select **Macro Control** from the Command drop down list.
3. When the related options are displayed, select the macro you want from the **Macro** drop down list and select a specific **Command** for the macro to perform.
4. When you're finished, click .

### *Assigning a Macro to a Door*

You can also assign a macro to a specific door by using the Simple Macro feature on the Door Operations page. For more information, see *Adding Simple Macros* on page 200 and *Operations tab (Mercury Security)* on page 243.

## Sorting Macros

By default, when you add macro commands, the command actions are activated in the order they are added. If you need to change the sequence of the macro commands, you can sort it into the order you want.

1. From the panel's Macros page, select the macro you want to sort.
2. On the following Macro Command  list, click **Sort**. This button only appears if you have two or more macro commands.

   Each of the macro commands are highlighted in gray.
3. Click and drag the macro commands into the order you want.
4. Click **Return** when you are done.

## Triggers

> **Note:** Only Mercury Security panels support triggers.

Triggers work with macros to generate a set of cause and effect events. Triggers are the specific sequence of events that must occur before a macro will be activated.

For example, you might define a trigger to be a tamper alarm issued by a specific subpanel. The macro linked to that trigger will then automatically lock the door associated with that panel and sound the alarm.

Triggers are usually defined through the Triggers  page on a specific panel or subpanel properties sheet.

### Adding Triggers

1. Select **Physical Access** > **Panels**.
2. Click the name of the panel that you want to add a trigger to.
3. On the Triggers page, click **Add New Trigger**.
4. Enter all the parameters that are required of the trigger.
5. Click  to save the new trigger.

### Editing Triggers

1. Select **Physical Access** > **Panels**.
2. Click the name of the panel that your trigger is on.
3. On the Triggers page, click the name of the trigger you want to edit.
4. On the following page, make the required changes.
5. Click  to save your changes.

### Deleting Triggers

1. Select **Physical Access** > **Panels**.
2. Click the name of the panel that your trigger is on.
3. On the Triggers page, click  for the trigger you want to delete.
4. When you see the confirmation message, click **OK**.

# Configuring Doors

Doors in the ACM system are logical units incorporating one or more components that are connected to a panel.

These components could include:

- Door, gate, elevator, escalator, etc.
- Lock (such as magnetic or strike) or relay
- Reader
- Keypad
- Contact
- Panic bar
- ACM Verify

These items do not need to be physically installed on a door, but should be included if they affect how the door locks or opens.

The usual components for a door are a reader, a lock (usually a strike), and a contact (usually a door position or DPOS) that reports the door state. Additionally you can have an exit button (request-to-exit or REX) on the opposite side of the door from the reader, or a second reader if you want to control access in both directions.

You can add doors:

- One at a time, configuring all settings manually.
- One at a time, configuring common or standardized door parameters and operational settings using a door template. You still need to configure many attributes such as operations, hardware, cameras, and interlocks specifically for individual doors. You must configure a door template before adding doors using that template.
- In bulk, when you add a new Mercury panel and use the Subpanel: Batch Create wizard to create the subpanels. At a minimum, you must have defined door templates with a Door Mode: option specified, to create doors with this wizard. You can use this wizard to create:
    - Subpanels with functioning doors. This requires door templates (to specify at least the Door Mode: option) and wiring templates (to assign addresses and input, output and reader templates to the doors).
    - Subpanels with non-functioning doors. This requires door templates (to specify at least the Door Mode:). You then need to complete the configuration for each door to make them all function.
    - Subpanels only. These can then be configured for doors or for inputs and outputs only, as needed.

  For more information about the templates you can use to create doors and subpanels, see *Templates Overview* on page 133. For more information about the Subpanel: Batch Create wizard, see *Batch Creating Subpanels on a New Mercury Panel* on page 161.

  See *Appendix: pivCLASS Configuration* on page 503.

## Searching for Doors

Many facilities require the control and monitoring of dozens, even hundreds, of doors simultaneously. This can result in a crowded listing page. You can search for specific doors to narrow the list of doors appearing on the Doors  list page.

1. Use any (or all) of the following to define your search:
    - Enter your search term in the **Search...** field. Use any series of letters and numbers to search for the doors you want to see.

- If known, select the **Device Status**.
- If known, select the **Appliance** the door is connected to.
- If known, select the **Group** the door is included in.

2. Click **OK**.

## Advanced Filtering on the Doors List

In addition to searching you can also use advanced filters to select multiple filters on the Door  list.

1. Click **Advanced Filters**.
   The Advanced Filters dialog box displays.
2. Select any required filters:
   - **Alarms**—Select the alarms to include from the list of alarms.
   - **Masked**—Select to include the masks to include from the list of masks.
   - **Normal**—Select to include all properly functioning doors.
   - **Door Mode**— Select the door modes to include from the list of door modes.

   **Note:** To unselect all selected filters, click **Unselect All**. All selections will be removed.

3. If you want to save the selected filters, select **Remember Filters**.
4. Click **OK**.

The Door  list refreshes to show the doors that meet your filters.

## Controlling Doors

While you are monitoring the system, you may need to override the default door settings to allow a visitor access to an area, or unlock a door in an emergency situation. From a Doors listing page in **Physical Access** or **Monitor** > **Dashboard**, use the Door Action, Door Mode, Forced, Held, and Installed drop-down menus to control doors.

Doors can also be controlled from **Monitor** > **Maps**. For more information, see *Using a Map* on page 432.

**Note:** Only the Installed options are available for virtual doors installed for use with ACM Verify readers.

1. Select the checkbox for each the door you want to control.
   Or click **All** at the top of the left column to select all doors or **None** to deselect all doors.
2. For one or more doors, select a **Door Action** if required:

   **Note:** The door actions below are not applicable for Schlage offline Wi-Fi doors or SALTO standalone doors. Only Grant is applicable for Schlage Control™ locks. Only Unlock and Locked No Access are applicable for Von Duprin remote undogging (RU) devices. Locked No

Access and Disable are not applicable for ASSA ABLOY battery-powered and external-powered doors.

- **Grant** — Momentarily grants access to the door to permit a single-time entry.
- **Restore** — Restores the Door Mode to its default configuration or Custom Mode.

  *Schlage locks with activated lock functions only.* Restoring a door that has an activated Lock Function (Classroom, Office, Privacy, or Apartment) removes the Lock Function and resets the door mode to its default configuration.

  *For ASSA ABLOY IP doors only.* Restoring a door results in the door going offline temporarily in the ACM system.
- **Unlock** — Unlocks the door. The door remains unlocked until the **Locked No Access** command is issued or until an operator override or scheduled action is initiated.
- **Locked No Access** — Locks the door. The door remains locked until the **Restore** command is initiated or until an operator override or scheduled action is initiated.
- **Disable** — Disables the door. The door stops operating and allows no access to anyone.
- **Lock (ASSA ABLOY Only)** — *For ASSA ABLOY IP doors only.* Locks the door. The door remains locked until a scheduled action is initiated.

3. Select any of the following **Door Mode** options to change the door mode.

   For more information, see *Door Modes* on page 203.
4. Select either of the following **Forced** options if required:
   - **Mask Forced** — Masks the Forced Door Alarm for the door. The status color changes to blue and is no longer included in any alarm subtotal.
   - **Unmask Forced** — Unmasks the Forced Door Alarm for the door.
5. Select either of the following **Held** options if required:
   - **Mask Held** — Masks the Door Held Open Alarm for the door.
   - **Unmask Held** — Unmasks the Door Held Open Alarm for the door.
6. Select either of the following **Installed** options if required:
   - **Install** — Installs a door. Enables communication between the door and the ACM system.
   - **Uninstall** — Uninstalls a door. Disables communication between the door and the ACM system.
7. Select **Delete** — Removes the connection between the door and the ACM system.

## Configuring Door Held-Open Settings

For Mercury Security and HID VertX doors.

Configure door settings for when a person enters or exits a door and does not close it in time. This may include sending a pre-alarm warning before the 'Door held open' event is generated.

1. Select **Physical Access** > **Doors**.
2. Select a door and then the **Operations** tab.
3. Enter:

| | |
|---|---|
| **Held Pre-Alarm** | The number of seconds a door can be held open before a pre-alarm is issued. If activated, the 'Door held open pre-alarm' event may be used to send an email notification.<br>Example: `20` seconds<br>If `120` seconds is entered in Held Open Time, the pre-alarm warning will be sent at 100 seconds and the 'Door held open' event at 120 seconds.<br>If `200` seconds is entered in Extended Held Open Time, the pre-alarm warning will be sent at 180 seconds and the 'Door held open' event at 200 seconds. |
| **Held Open Time** | The number of seconds a door can be held open before a 'Door held open' event is generated.<br>Example: `120` seconds |
| **Extended Held Open Time** | The number of seconds a door can be held open for users with extended access permissions before a Door held open' event is generated.<br>This feature is useful for users that may require more time to enter a door, such as individuals with accessibility needs.<br>Example: `200` seconds |

To enter other door configuration, see *Operations tab (Mercury Security)* on page 243 or *Operations tab (VertX®)* on page 229.

4. Click ✔.

## Adding Doors

To add a new door:

1. Select **Physical Access** > **Doors**.

> **Note:** Doors cannot be manually added for Allegion offline Wi-Fi locks, SALTO doors and ASSA ABLOY IP doors. For information about adding doors and associated panels, see *Step 2: Setting Up Communication to Offline Wi-Fi Locks* on page 277, *Step 3: Syncing Doors with the SALTO Server* on page 286 and *Step 2: Syncing Doors with the Door Service Router* on page 296, respectively.

2. Click **Add Door**.
3. If door templates are used, the Templates dialog appears. To use the door settings from a template, which automatically fills in the fields on the Parameters and Operations tabs, select the template and click **OK**. Otherwise, click **Cancel**.

   For Schlage IP-mode wireless devices or devices connecting to an RS485 hub, click **Cancel**.
4. Enter on the **Parameters** tab:

> **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| | |
|---|---|
| **Name** | Up to 50 characters for the name of the door. See *Appendix: pivCLASS Configuration* on page 503. |
| **Alt. Name** | An alternate name for the door. |
| **Location** | A short description of the door location. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | The panel that controls the door, the gateway that controls the IP-mode wireless device or the offline Wi-Fi device, or the external server that the ACM appliance is connected to. |
| | Displays for a panel that is connected to a subpanel that controls readers, locks, inputs and outputs; or a gateway that controls IP-mode wireless devices.<br>**Subpanel**: The name of the subpanel that is connected to the main panel or the name of the gateway.<br>**Door Number** or **Lock Number**: The door number for wired connections or lock number for wireless devices. For SimonsVoss wireless locks, use the hexadecimal address assigned by the SmartIntego Tool.<br>**Device Id**: Displays for Aperio AH-40 Hub subpanel only. The Lock/Sensor identifier from the Aperio programming application. |
| | Displays for a Schlage ENGAGE Gateway.<br>**Lock Model**: The lock model from the vendor.<br>**Linked Device**: The ID or name of each externally commissioned IP wireless or offline Wi-Fi device. For more information, refer to the commissioning process in vendor documentation. |
| | Displays for an ASSA ABLOY DSR.<br>**Lock Type**: The battery-powered or external-powered lock type from the vendor.<br>**Serial Number**: The serial number of the lock. |
| **Appliance** | The ACM appliance that is connected to the door, gateway, hub or external server. |
| **Vendor** | The manufacturer of the panel, gateway, offline Wi-Fi device or external server. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |

Displays for **Schlage** ENGAGE Gateway subpanel:

**Access Type**: Displays for an IP-connected wireless device only. Whether access is located on one or both sides of the door. Default is **Single**, which cannot be changed. For more information, see *Access Types* on page 204.

**Door Mode**: IP-connected wireless device only. The entry mode for the door when the gateway is online and communicating with the device. For information about the **Unlocked**, **Locked No Access** and **Card Only** options, see *Door Modes* on page 203.

*IP-connected RU exit device only (not applicable to RM).* The entry mode for the door when the gateway is online and communicating with the device. For more information about the **Unlocked** and **Locked No Access (Unlocked on Next Exit)** options, see *Door Modes* on page 203.

*Offline Wi-Fi lock only.* The entry mode for the door when the lock is online. For information about the **Card Only** option, see *Door Modes* on page 203.

**Lock Function**: None is the default (not applicable to RM device).

- **None**: Use the system default door settings.
- **Privacy**: When the interior lock button is pressed, the door will lock and the exterior lock will not grant access to any token. To unlock the door, the interior lock button must be pressed again or exit the room.

  **Note:** Only this lock function is supported for the ASSA ABLOY IP locks.

- **Apartment**: Use the interior lock button to toggle between locked and unlocked. When the door is locked, any valid token will open the door. The door must be manually locked or it will stay unlocked.
- **Classroom — Classroom/Storeroom** — The lockset is normally secure. The inside lever always allows free egress. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may be used to change to a passage or secured status. Not to be used on mortise deadbolt. Interior push button not to be used.

  **Note:** Only this lock function is supported for the RSI-connected NDE series lock.

  **Note:** This lock function is not supported for the IP-connected LE, LEB, NDE and NDEB series lock, or offline Wi-Fi lock.

- **Office** — The lockset is normally secure. The inside lever always allows free egress. An interior push-button on the inside housing may be used to select a passage or secured status. Meets the need for lockdown function for safety and security. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may also be used to change status. Not to

| | |
|---|---|
| | be used on mortise deadbolt.<br><br>**Note:** A Restore door action is available on the Door listing page and the Hardware Status page which resets the Door Mode to its default value.<br><br>**Always Mask Forced**: If selected, Door Forced Open alarms at the door are always masked.<br><br>**Always Mask Held**: If selected, Door Held Open alarms at the door are always masked.<br><br>**Custom Mode**: Another door mode that is supported by the gateway.<br><br>**Custom Schedule**: Displays for an IP-connected door (LE, LEB, NDE, NDEB series lock) if the Card Only door mode is selected, or IP-connected RU device if the Locked No Access door mode is selected. A predefined time when Custom Mode becomes active. **Never Active** is OFF. **24 Hours Active** is ON. |
| | For **Avigilon**, enter:<br><br>**Station Type**: Default is **ACM Verify** station, which is used on connected devices. A device that uses this station type of station is called an ACM Verify Station.<br><br>**Managed**: If selected, ACM Verify Station requires the user to grant or deny access to the person entering a valid PIN code. It also displays the name and picture of the user for verification.<br><br>**UnManaged**: If selected, ACM Verify Station automatically grants or denies access and does not provide additional information when a PIN code is entered.<br><br>**Geographic Timezone**: The time zone where the ACM Verify device is located if it is different from the time zone of the ACM appliance.<br><br>**Into Area**: The area that the badge holder enters by passing through the door and where the ACM Verify Station is used, or not, to monitor access to the area. You must specify an area if you want the virtual station to list all the people who have entered the area.<br><br>**Station Authentication**: The method of authentication on the ACM Verify device. **Login** specifies that the user log in to the ACM software using the ACM URL from the browser on the ACM Verify device. **Paired** specifies that the ACM Verify is paired to the ACM system. If the authentication type is Paired, the Door Add page refreshes and displays the Add Paired Device button.<br><br>**Tip:** The Avigilon settings do not require a panel. |

| | |
|---|---|
| | For **Mercury Security** and **HID** VertX panel, enter:<br>**Access Type**: Whether the reader is located on one or both sides of the door, or on an elevator door. See *Access Types* on page 204.<br>**Linked Door**: Displays for **Paired Primary** and **Paired Replica** access type only. The door with the reader on the other side of the door.<br>**Door Mode**: The entry mode of the door when the door controller is online and communicating with the panel. See *Door Modes* on page 203.<br>**Assurance Profile**: For Mercury Security LP4502 only. See *Appendix: pivCLASS Configuration* on page 503.<br>**Offline Door Mode**: The entry mode of the door if the door controller is no longer communicating with the panel.<br>**Note:** In many cases readers in offline mode require a very simple solution for entry or exit because of the memory limitations. The recommended Offline Door Mode option is **Locked No Access**.<br>**Custom Mode**: Another entry mode that is supported by the door module in addition to Door Mode and Offline Door Mode options.<br>**Custom Schedule**: When the Custom Mode becomes active. Never Active is OFF. 24 Hours Activeis ON.<br>**Masked Forced Schedule**: A predefined time when Door Forced Open alarms from the door will be masked.<br>**Masked Held Schedule**: A predefined time when Door Held Open alarms from the door will be masked.<br>**Always Mask Forced**: If selected, Door Forced Open alarms at the door are always masked.<br>**Always Mask Held**: If selected, Door Held Open alarms at the door are always masked. |
| | For **SALTO** panel, enter:<br>**Door Mode**: The entry mode of the door after syncing with the SALTO server and installing the door. See *Door Modes* on page 203.<br>**Custom Mode**: Another entry mode of the door that is time-based (see Custom Schedule). Can be **Unlocked**, **Card and Pin**, **Office**, **Toggle** or **Keypad Only**. If Keypad Only is selected, **Keypad Code** is displayed. You can enter up to 8 digits. See *Door Modes* on page 203.<br>**Custom Schedule**: A predefined time when Custom Mode becomes active.<br>**Always Mask Forced**: If selected, Door Forced Open alarms at the door are always masked.<br>**Always Mask Held**: If selected, Door Held Open alarms at the door are always masked. |

| | |
|---|---|
| **Door Processing Attributes** | For **Schlage** door, select:<br><br>**Note:** The following three attributes are not applicable to Control locks or offline Wi-Fi locks.<br><br>**Log Grants Right Away**: Initiates local I/O in the panel using the panel triggers. The system logs an extra event as soon as a grant occurs (that is, before entry / no entry is determined). This event is not turned into an Access Control Manager event.<br><br>Certain customers may have a trigger they want to fire (to execute a macro) as soon as there is a grant but before entry / no entry is determined.<br><br>**Log All Access as Used**: Logs all access grant transactions as if the person used the door. If this field is not selected, the door determines if it was opened and distinguishes if the door was used or not used for grant.<br><br>**Detailed Events**: Displays the current position of the door position switch (DPOS) in the Door State column of the door listing screen. When enabled the column displays “Open” when the DPOS is in an open state and “Closed” when the DPOS is in a closed state.<br><br>**Note:** To properly report the Door State from the Door Position Switch, Detailed Events must be enabled.<br><br>Typically, five to ten detailed transactions are generated for each grant transactions. During the normal course of operation, most guards don't need to see extensive reports on events; however, after hours, it is often useful to see every detail.<br><br>**Do Not Log Rex Transactions**: Indicates that request-to-exit transactions do not get logged to the database.<br><br>**Note:** This is the only attribute supported for offline Wi-Fi locks. |

For **Mercury Security** panel, select:

**Log Grants Right Away**: Initiates local I/O in the panel using the panel triggers. The system logs an extra event as soon as a grant ocurs (that is, before entry / no entry is determined). This event is not turned into an Access Control Manager event.

Certain customers may have a trigger they want to fire (to execute a macro) as soon as there is a grant but before entry / no entry is determined.

**Deny Duress** : Denies access to a user that indicates duress at a door.

**Don't Pulse Door Strike on REX**: Disables the pulse of the door strike output when the request-to-exit button is pressed and can be used for a 'quiet' exit. If not selected, the output is pulsed.

> **Note:** This field must not be checked for the SimonsVoss wireless lock, such as cylinders, on a door that does not support a door position switch (DPOS).

**Require Two Card Control**: Two tokens are required to open this door. This enforces the two-person rule at a specified door.

**Door Forced Filter:** : Filters door-forced alarms. Sometimes a door is either slow to close or is slammed shut and bounces open for a few seconds. With this filter, the monitor allows three seconds for a door to close before issuing an alarm.

**Log All Access as Used**: Logs all access grant transactions as if the person used the door.  If this field is not selected, the door determines if it was opened and distinguishes if the door was used or not used for grant.

**Detailed Events**: Displays the current position of the door position switch (DPOS) in the Door State column of the door listing screen. When enabled the column displays “Open” when the DPOS is in an open state and “Closed” when the DPOS is in a closed state.

> **Note:** To properly report the Door State from the Door Position Switch, Detailed Events must be enabled.

Typically, five to ten detailed transactions are generated for each grant transactions. During the normal course of operation, most guards don't need to see extensive reports on events; however, after hours, it is often useful to see every detail.

**Enable Cipher Mode**: Enables the operator to enter card number digits at the door’s keypad.

**Use Shunt Relay**:Enables the use of a shunt relay for this door.

**Do Not Log Rex Transactions**: Indicates that request-to-exit transactions do not get logged to the database.

| | |
|---|---|
| | For **HID** VertX panel, select:<br>**Door use Tracking**: The level of door event tracking that is logged in the Monitor screen. These options should only be used when the **Detailed Events** option is enabled.<br>• **None**: Only standard door events are logged.<br>• **Used**: The details of when the door is used.<br>• **Used with pending**: The events that occur between door use.<br>**Deny Duress**: If selected, denies access to a user who is in duress at a door.<br>**Don't Pulse Door Strike on REX**: Disables the pulse of the door strike when request-to-exit button is activated.<br>**Detailed Events**: For circumstances when it is important to know all the details of an event. Displays the current position of the door position switch (DPOS) in the Door State column of the Door list. When enabled the column displays "Open" when the DPOS is in an open state and "Closed" when the DPOS is in a closed state.<br>**Enable Cipher Mode**: Allows the operator to enter card number digits at the door's keypad.<br>**Do Not Log Rex Transactions**: Disables logging of request-to-exit transactions. |
| | For **SALTO** panel, select:<br>**Detailed events**: Enables the reporting of event details, such as Door State and Door Mode, after syncing and installing the door.<br>**Do Not Log Rex Transactions**: Disables logging of request-to-exit transactions. |

5. Click ✔ to add the door. Once saved the page becomes the Door: Edit page. If a door template was used, the fields on the Parameters and Operations tabs are entered.
6. To edit door configuration, see *Editing Doors* on the next page. To edit lock configuration, see *Step 3: Configuring IP-enabled Wireless Devices* on page 269.
   - **Parameters**: Edit access type, processing attributes, lock functions, and other options.
   - **Operations**: Displays for HID VertX, Mercury Security, Schlage wired and RSI wireless locks, and ASSA ABLOY IP locks only. Edit simple macros, accepted card formats and other options.
   - **Hardware**: Displays for HID VertX, Mercury Security, and Schlage wired and RSI wireless locks only. Edit reader, door position, strike and request to exit (REX).
   - **Elev**: Displays for Mercury Security only. View elevator door details.
   - **Cameras**: Add or remove associated cameras.
   - **Interlocks**: Displays for Mercury Security only. Sets interlocks.
   - **Events**: View and edit door events.
   - **Access**: Does not display for RU and RM exit devices. View access groups, roles and identities that have door access.
   - **Transactions**: View door transactions.
   - **Notes**: Add notes about the door and review previous notes, if any.
7. Click ✔ to save your changes.

## Adding Simple Macros

You can add simple macros, or single action commands, to any door in the system. Simple macros are triggered by one type of door event. This automatically activates the corresponding output.

For more information about macros, see *Macros* on page 186.

1. Select **Physical Access**.

   The Door  list is displayed.
2. Select a door from the Door  list.
3. On the Door Edit screen, select the **Operations** tab.

   At the bottom of the page is the Simple Macros section.
4. Select the **Type** of door event that will activate the output. The options are:
   - Forced
   - Held
   - Pre-Alarm
5. Select when the simple macro will be active from the **Schedule** drop down list. Only schedules that have been configured in the system are listed.
6. Select the output that is activated when the selected type of door event is triggered.
7. Click **Save Macro**.

   A new row is automatically added to the table.
8. If you need to add another simple macro, repeat steps 4 - 7 in the new row.

   To remove a configured simple macro, simply click **Remove Macro**. The row is deleted.
9. Click  to save your changes.

## Editing Doors

A door can be edited after its initial configuration. For example, you may need to change the access type or door mode to reflect changes on your site.

1. Select **Physical Access** > **Doors**.
2. Select the name of the door.
3. Edit the details on each tab as required:
   - **Parameters**: Edit access type, processing attributes, lock functions, and other options.
   - **Operations**: Displays for HID VertX, Mercury Security, Schlage wired and RSI wireless locks, and ASSA ABLOY IP locks only. Edit simple macros, accepted card formats and other options.
   - **Hardware**: Displays for HID VertX, Mercury Security, and Schlage wired and RSI wireless locks only. Edit reader, door position, strike and request to exit (REX).
   - **Elev**: Displays for Mercury Security only. View elevator door details.
   - **Cameras**: Add or remove associated cameras.
   - **Interlocks**: Displays for Mercury Security only. Sets interlocks.
   - **Events**: View and edit door events.
   - **Access**: Does not display for RU and RM exit devices. View access groups, roles and identities that have door access.
   - **Transactions**: View door transactions.
   - **Notes**: Add notes about the door and review previous notes, if any.

   For field descriptions, see:
   - VertX on page 227
   - Mercury Security on page 239

- Schlage IP wireless locks, and RU or RM devices on page 270
- SALTO doors on page 287
- ASSA ABLOY IP doors on page 297

4. After editing each tab, click to save your changes.

### Doors - Editing VertX® Doors

1. Select **Physical Access**.
   The Doors list is displayed.
2. From the Doors list, click the VertX® door name you want to edit.
   The Door: Edit screen for that specific door type is displayed.
3. Optional: Add notes about the door and review previous notes, if any.
4. Edit the door by changing values on each of the door option tabs.
5. When you're finished, click .
   You are returned to the list with all changes saved.

### Doors - Editing Mercury Security Doors

To edit an existing Mercury Security door:

1. Select **Physical Access**.
   The Doors list page is displayed.
2. Click the door name to select the door you want to edit.
   The Door Edit screen for that specific door is displayed.
3. Optional: Add notes about the door and review previous notes, if any.
4. When you're finished, click .

   You are returned to the list with all changes saved.

## Deleting Doors

To delete a door:

1. From the Door list, click for the door that you want to delete.
2. When the confirmation message appears, click **OK**.
   The selected door is now removed from the system.

> **Note:** *SALTO doors only.* When doors are deleted in the ACM system, the corresponding doors in the SALTO system are not deleted. At the next manual sync in the ACM system, the door will display as a new uninstalled door.

# Door Modes

**Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

*For Mercury Security and HID VertX panels.* The same list of options is provided for the Offline Door Mode option.

*For ASSA ABLOY IP-enabled doors, SALTO standalone doors and Schlage offline Wi-Fi doors*. Any locks that do not support real-time communication with a server, will not display door mode options on the Doors list page and maps. Door mode can be set on the Door: Edit page and by using a batch job (specification).

| Door Mode | Description |
|---|---|
| **Disabled** | The door is disabled for all access. |
| **Unlocked** | The door is always unlocked. |
| **Locked No Access** | The door is always locked. No access is allowed through this system. |
| **Locked No Access (Unlocked on Next Exit)** | The door is locked until a person presses the push bar to exit. |
| **Facility Code Only** | The door can be accessed using a facility code.<br><br>All employees share a single code. This option can be useful in offline situations, when the door controller is no longer communicating with the Access Control Manager host.<br><br>*Mercury door only.* The Offline Door Mode is no longer supported if the door controller is connected to an LP4502 panel that has replaced an HID VertX panel. |
| **Card Only** | The door can be accessed using a card. No PIN is required. To support the selected **Assurance Profile** for a pivCLASS configured door, it is recommended to set the Door Mode to **Card Only**.<br><br>*Mercury door only.* The type of reader used to read this card is determined in the Reader Type field. |
| **Pin Only** | The door can only be accessed by entering a PIN at a keypad.<br><br>No card is required.<br><br>**Note:** This door mode is not available if the 'Allow duplicate PINs' option has been selected on the System Settings - General page. |
| **Card and Pin** | The door can only be accessed using both a card and a PIN.<br><br>*ASSA ABLOY IP door only.* If the token does not have a PIN, the door can be accessed by swiping the card only. |

| Door Mode | Description |
|---|---|
| **Card or Pin** | The door can be accessed either by entering a PIN at a keypad or by using a card at the card reader.<br><br>**Note:** This door mode is not available if the 'Allow duplicate PINs' option has been selected on the System Settings - General page. |
| **Office** | *SALTO door only*. The lock allows the cardholder to leave the lock open.<br><br>To use this mode, the cardholder presents the key to the door while pressing down the inner handle and repeats the procedure to undo the mode. |
| **Toggle** | *SALTO door only*. The door allows the cardholder to toggle between leaving the lock open and closing it by presenting the assigned key (there is no need to press down the inner handle).<br><br>To use this mode, the cardholder presents the key to leave the lock open and repeats the procedure to close it. |
| **Keypad Only** | *SALTO door only*. The door can only be accessed by entering the shared keypad code at a keypad. If selected, Keypad Code is displayed. You can enter up to 8 digits. |
| **First Person Through** | *ASSA ABLOY battery-powered or external-powered door only*. The first person who is granted access to the door will unlock the lock. |
| **Exit Leaves Open** | *SALTO door (not connected to control unit) only*. The door is unlocked when the inner door handle is pressed. Allows the cardholder to exit and return to the building without using an assigned key during an emergency (referred to as Escape and Return mode).<br><br>To lock the door, add a global action to set a time limit on the open door. |
| **Toggle and Exit Leaves Open** | *SALTO door (not connected to control unit) only*. The door allows the cardholder to use either the Toggle or Exit Leaves Open door mode during an emergency (referred to as Escape and Return mode). |

## Access Types

When you select an Access Type from the Door Edit page, the listed options include:

**Note:** The options may be different depending on the type of panel that is connected to the door.

| Feature | Description |
|---|---|
| **Single** | This is a door with a reader/keypad on only one side, normally entry only. |
| **Paired Primary** | This indicates that this door possesses a reader/keypad on both sides, entry and exit, and that this side is the Primary.<br><br>If you select this option, the **Paired Door** option is automatically displayed for you to specify the other reader that is installed on the door. |

| Feature | Description |
|---|---|
| **Paired Replica** | This indicates that this door possesses a reader/keypad on both sides, entry and exit, and that this side is the replica.<br><br>If you select this option, the **Paired Door** option is automatically displayed for you to specify the other reader that is installed on the door. |
| **Elev no feedback** | This door is an elevator with no feedback input. |
| **Elev feedback** | This door is an elevator with a feedback input. |

# Anti-Passback

The anti-passback (APB) feature can be configured to log or prevent a card from being re-used to access the same area unexpectedly.

For example, the same card cannot be used to enter the same room twice in a row. If a badge holder enters a room then passes the card to another potential badge holder to reuse the card at the same door, an APB error is logged and may be configured to prevent the second badge holder from entering.

Another example is when an access card is also required to exit. If a badge holder holds open a door for another person, the second person would not be able to exit even if they have an access card because the system requires the badge holder to log an entrance in the system before they can exit.

To set up this feature, complete the following procedures:

## Anti-Passback Modes

When you select the Operations  tab on the Door Edit page, one of the options is **APB Mode**.

Anti-Passback (APB) requires that a user must enter and exit a room before they may enter another room. For example, the typical user of a parking lot would normally swipe their card at the “in” reader to enter the lot and swipe it at the “out” reader to exit the lot. However, if a user swipes their card at the “in” reader then passes their card back to a friend, the card would be denied access the second time when it is swiped by the friend.

To track anti-passback, a card reader must be installed on both the inside and the outside of the door. Users are required to use the card to enter and exit the building.

**Note:** The APB modes may be different depending on the panels you have installed.

| Mode | Description |
|---|---|
| **No Selection** | APB is not used. |

| Mode | Description |
|---|---|
| **Door-Based Timed APB** | Allows you to configure APB with just one reader. The door keeps track of each badge that enters and does not allow the same badge to enter twice in a row until after the APB time limit is reached.<br><br>Make sure you specify an APB time limit in the **APB Delay** field. Do not configure the area entering or area leaving setting for the door.<br><br>**Note:** This mode is only available if using Mercury Security hardware. For more information, see *Panel Migration* on page 156. |
| **Token-Based Timed APB** | Tracks each door a badge has accessed. After the badge has accessed one door, it must access a second door or wait until the APB time limit is reached before it may access the first door again.<br><br>Make sure you specify an APB time limit in the **APB Delay** field. Do not configure the area entering or area leaving setting for the door.<br><br>**Note:** This mode is only available if using Mercury Security hardware. |
| **Hard Door APB** | Tracks each badge that enters a door and does not allow the same badge to enter twice in a row. This badge will not be able to enter through the same door until it has accessed a second door.<br><br>Enter a value in the **APB Delay** field to create a time-based APB.<br><br>**Note:** This mode is only available if using VertX® hardware. For more information, see *Panel Migration* on page 156. |
| **Soft Door APB** | Tracks each badge that enters a door and generates a warning transaction if the same badge is used at the same door twice in a row. This badge is still able to enter the door the second time, but the access is logged as an APB violation.<br><br>Enter a value in the **APB Delay** field to create a time-based APB.<br><br>**Note:** This mode is only available if using VertX® hardware. For more information, see *Panel Migration* on page 156. |

| Mode | Description |
|---|---|
| **Hard Area APB** | Tracks each badge that enters a specific area and defines which areas the badge may access next. The badge is denied access if it tries to access an undefined area. If the badge is used to access an area that a person is already in, the badge is denied access and an APB violation is logged.<br><br>Enter a value in the **APB Delay** field to create a time-based APB.<br><br>Make sure you configure the area entering and area leaving setting for the specified door.<br><br>**Note:** The Don't Care setting is not applicable to the Out of Area and Into Area fields. In addition, this mode is not used across multiple controller panels. |
| **Soft Area APB** | Tracks each badge that enters a specific area and defines which areas the badge may access next. The badge is allowed to access the area, but the access is logged as an APB violation.<br><br>Enter a value in the **APB Delay** field to create a time-based APB.<br><br>Make sure you configure the area entering and area leaving setting for the specified door. |
| **Timed Area APB** | Time-based hard area APB. When the time limit expires, the hard area APB becomes a soft area APB. If a person leaves the area by going through a door marked Out of Area, the APB will be reset.<br><br>Enter a value in the **APB Delay** field to create a time-based APB.<br><br>Make sure you configure the area entering and area leaving setting for the specified door.<br><br>**Note:** This mode is only available if using Mercury Security hardware. |

## Setting Up Anti-Passback

Before you begin, consider what type of anti-passback (APB) mode that you need for each situation. For more information, see *Anti-Passback Modes* on page 205.

To use the APB feature, you must set up at least two doors in ACM: one to represent the entrance and one to represent an exit.

**Note:** All doors should use the same controller panel for best results. For information about two-person minimum occupancy on an installed door that uses Mercury panels and controller firmware 1.29.1 or later, see *Two-Person Minimum Occupancy and Single Door Configuration* on the next page.

1. Create at least one area.
2. Create two doors that are connected to the same panel.
    - If there are two distinct doors in the room (for example, a door on opposite ends of a room), select **Single** as the Access Type.
    - If there is only one door in the room, you still must create two doors in the system. For the entrance door, select **Paired Primary** as the Access Type. This door will control all the inputs and outputs that are connected to the door.

      For the exit door, select **Paired Replica** as the Access Type. This door will only control the reader that allows badge holders to exit the room.

      For both doors, assign the other door as the **Linked Door**.
3. After the doors have been created, assign an **APB Mode** for each door on the door's Operations tab.

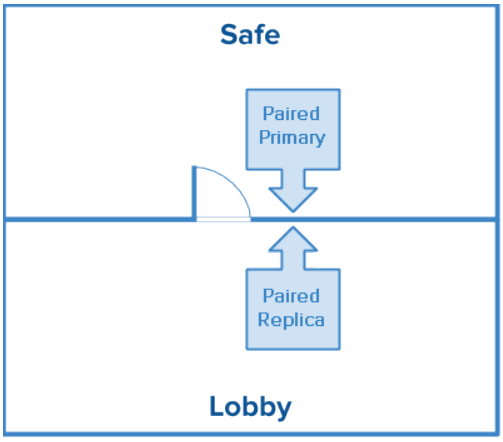
   Remember to click to save the changes on each page.
4. Assign the area you created in the first step for the **Into Area** for each door.
5. If you created more than one area, select the **Out of Area** for each door. Otherwise, you can leave it as **Don't Care**.
6. If you are setting up a timed APB mode, enter the number of seconds before another entry is allowed in the **APB Delay** field.

***Two-Person Minimum Occupancy and Single Door Configuration***

Mercury Security doors only.

> **Note:** Two-person minimum occupancy is supported on an installed door that uses Mercury panels and controller firmware 1.29.1 or later.

An area with 2-Person Control enabled in ACM (see Safe in the following example) will enforce a two-person occupancy minimum in the area. This means that the first access requires two people to swipe their cards before they can access the area. Any subsequent access requires only one person to swipe their card. When leaving the area, the last two people need to swipe their cards in order to exit.




To configure a two-person minimum occupancy area and door access for two or more identities and their tokens:

1. Add and edit two areas in ACM.

   Example:

   Control area:

| Name | Enable Area | 2-Person Control | Doors In | Doors Out |
|---|---|---|---|---|
| Safe | ☑ | ☑ | Safe Entry | Safe Exit |

   Adjacent lobby:

| Name | Enable Area |
|---|---|
| Lobby | ☑ |

   For more information, see *Adding Areas* on page 301 and *Editing Areas* on page 301

2. Add two doors in ACM to represent the single Mercury Security door.

   Example:

   Door representing the entry into the two-person minimum occupancy area:

| Name | Installed | Access Type | APB Mode | Into Area | Out of Area |
|---|---|---|---|---|---|
| Safe Entry | ☑ | **Paired Replica** | **Hard Area APB** | Safe | Lobby |

   **Hardware** tab:

| Door Position | Strike |
|---|---|
| (not selected) | (not selected) |

   Door representing the exit from the two-person minimum occupancy area:

   **Operations** tab:

| Name | Installed | Access Type | APB Mode | Into Area | Out of Area |
|---|---|---|---|---|---|
| Safe Exit | ☑ | **Paired Primary** | **Hard Area APB** | Lobby | Safe |

   **Hardware** tab:

| Door Position | Strike |
|---|---|
| Safe Exit DPOS (Subpanel:*N* Output:*N*) | Safe Exit Strike (Subpanel:*N* Output:*N*) |

   For more information, see *Adding Doors* on page 214 and *Editing Doors* on page 201.

3. Add two or more identities and ensure their tokens are assigned. For more information, see *Adding an Identity* on page 65 and *Assigning Tokens to Identities* on page 67.

   If specified, **APB Exempt** applies to all defined areas.

4. To enter the two-person minimum occupancy area:
   - If the area is empty, two people will need to swipe their individual cards to access the area. The second card must swipe within 15 seconds of the first swipe.
   - When the area contains two people, a swipe from a third person (and any subsequent swipe) will allow access to the area.

5. To leave the two-person minimum occupancy area:
    - If the area contains more than two people, a single swipe will allow them to exit the area until only two people are left in the area.
    - When the area contains only two people, both of them will need to swipe to exit the area. The second card must swipe within 15 seconds of the first swipe.

### Granting a Free Pass

You can grant a user one free pass to enter a door without generating an anti-passback error. This feature is useful if a badge holder swiped their card at a card reader but did not actually enter the area.

For example, an employee uses his access card to unlock the office entrance but is distracted by another employee before he opens the door. The two employees speak for several minutes, and the door automatically locks after a set amount of time. When the first employee attempts to unlock the office door again, this triggers an APB alarm and the employee is locked out. The employee contacts the security officer and explains the situation, the security officer can grant one free pass to allow the employee back into the office area.

To grant a free pass:

1. Click **Identities**.

   The Identities  list is displayed.
2. From the Identities  list, click on the name of the identity.

   The Identities: Edit screen is displayed.
3. Select the **Tokens** tab.
4. Beside the **1 free pass** button, select a door.
5. Click **1 free pass**.

   The badge holder can now enter the door without generating an new anti-passback alarm.

### Global Anti-Passback

Global anti-passback defines an area for which two or more readers are used to access the area, but are physically wired to different controllers. If any one reader in that same area receives an APB violation, it will prevent that badge holder from entering through other doors in same area.

#### *Global Anti-Passback Modes*

Global anti-passback is automatically implemented using APB mode. For more information about global anti-passback modes, see *Anti-Passback Modes* on page 205.

## Interlocks

> **Note:** Only Mercury Security doors support interlocks.

An interlock is a mechanism that enables a specific event from one element of the system to trigger an action at another element. Interlocks allow you to set up security routines like man-traps, prison entry points, and automated building functions.

The interlock feature can be accessed from one of three ways:

Accessing Interlocks through Doors

1. Select **Physical Access**.
   The Doors  list is displayed.
2. Select the Mercury Security door that you want to interlock.
   The Door Edit screen is displayed.
3. Click the **Interlocks** tab.
   The Door Interlocks  list is displayed.

Accessing Interlocks from Subpanel Inputs

1. Select **Physical Access**>**Panels**.
   The Panels  list is displayed.
2. Select the panel you want to interlock.
   The Panel Status screen is displayed.
3. Click the **Subpanels** tab.
   The Subpanels  list is displayed.
4. Click  for the subpanel that is connected to the input you want to interlock.
   The Inputs  list is displayed.
5. Click the **Interlocks** link beside the required input.
   The Input Interlock  list is displayed.

Accessing Interlocks from Subpanel Outputs

1. Select **Physical Access**>**Panels**.
   The Panels  list is displayed.
2. Select the panel you want to interlock.
   The Panel Status screen is displayed.
3. Click the **Subpanels** tab.
   The Subpanels  list is displayed.
4. Click  for the subpanel that is connected to the output you want to interlock.
   The Outputs  list is displayed.
5. Click the **Interlocks** link beside the required output.
   The Output Interlock  list is displayed.

## Adding Interlocks

1. From the Interlock  list, click **Add Interlock**. For more information about how to access the different Interlock Listing pages, see *Interlocks* on the previous page.
2. On the following Interlock Add page, add the required information.
   Notice that as you select options, new fields are displayed to help you further define your requirements.
3. When you're finished, click  to save the new interlock.

### Editing Interlocks

1. From the Interlock  list, click the name of an interlock. For more information about how to access the different Interlock Listing pages, see *Interlocks* on page 210.
2. On the following Interlock Edit page, make the required changes.
3. Click to save your changes.

## Doors list

The **Doors** page lists of all the doors you are authorized to see and control. From this list you can control doors, as well as add and delete doors, edit doors and their associated controller panels, and create overrides to temporarily change the normal status of selected doors.

> **Note:** Overrides can only be applied to installed doors on Mercury panels using controller firmware 1.27.1 or later.

Select **Physical Access** > **Doors** to access the Doors list.

You can add notes about the doors list and review previous notes, if any. These notes are unique to the entire list of doors and are not partitioned.

**Searching, sorting, and filtering**

Many facilities require the control and monitoring of dozens, even hundreds, of doors simultaneously. This can result in a crowded listing page. You can search for specific doors to narrow the list of doors, filter the columns for specific values, and create and save custom filters. You can then sort the results using any one column.

**Searching the list:**

1. Use any (or all) of the following to define your search:
   - Enter your search term in the **Search...** field. Use any series of letters and numbers to search for the doors you want to see.
   - If known, select the **Device Status**.
   - If known, select the **Appliance** the door is connected to.
   - If known, select the **Group** the door is included in.
2. Click **OK**.

**Creating a filter to select multiple filters:**

1. Click **Advanced Filters** to open the Advanced Filters dialog box.
2. Select filters:
   - **Alarms**—Select the alarms to include from the list of alarms.
   - **Masked**—Select to include the masks to include from the list of masks.
   - **Normal**—Select to include all properly functioning doors.
   - **Door Mode**— Select the door modes to include from the list of door modes.

   To unselect all selected filters, click **Unselect All**.
3. If you want to save the selected filters, select **Remember Filters**.
4. Click **OK**.

**Sorting the list:**

1. Click in a column heading:
    - Click ▲ to sort in ascending order.
    - Click ▼ to sort in descending order.

**To see the legend for all the device statuses:**

- Click **Legend** to see the list of statuses and the related icons.

  There are three groupings which are color-coded — Normal ✓, Alarms ●, Masked ●:

**Adding and deleting doors**

- Click the **Add Door** button to define a new door. For more information, see *Adding Doors* on the next page.
- Select doors in the list and click the **Delete** button.

**Editing doors and panels:**

- Click the link to the door in the **Name** column. For more information, see *Editing Doors* on page 201.
- Click the link to the panel in the **Panel** column.

**Controlling doors:**

Select doors in the list and then use the drop-down options from the control buttons at the top of the page to control them:

- **Door Action**
- **Door Mode**
- **Forced**
- **Held**
- **Installed**

For more information, see *Controlling Doors* on page 191.

**Creating a Door Configuration report**

- Click **Create New Report** to generate a Door Configuration report on the doors in this list.

The following information is displayed for each door in the list:

| Column Heading | Description |
|---|---|
| **All/None** | Use this toggle to select and deselect all the doors currently visible in the list. Or you can use the checkbox to select individual doors. |
| **Device status** | Displays the device status. Hover the mouse over the related icon to see more details.<br><br>**Note:** The tamper icon only appears for OSDP readers, and reports whether the reader is offline or has been tampered with. |
| **Name** | The name assigned to this door.<br><br>Click on this name to open the Door: Edit page Parameters tab. |

| Column Heading | Description |
|---|---|
| **Panel** | The name of the panel to which this door is connected. Click on this name to open the Panel: Edit page Configure tab. |
| **Door state** | Current state of the related door: Open or Closed.<br><br>**Note:** To properly report the Door State from the Door Position Switch, the Detailed Events parameter must be enabled for the door. If this parameter is not set for a door, edit the parameters for the door. |
| **Door mode** | Indicates the door mode — the method by which the door is opened:<br>• Disabled<br>• Unlocked<br>• Locked No Access<br>• Facility Code Only<br><br>**Note:** The Offline Door Mode is no longer supported if the door controller is connected to an LP4502 panel that has replaced an HID VertX panel.<br><br>• Card Only<br>See *Appendix: pivCLASS Configuration* on page 503.<br>• Pin Only<br>• Card & Pin<br>• Card or Pin |

## Adding Doors

To add a new door:

1. Select **Physical Access** > **Doors**.

   **Note:** Doors cannot be manually added for Allegion offline Wi-Fi locks, SALTO doors and ASSA ABLOY IP doors. For information about adding doors and associated panels, see *Step 2: Setting Up Communication to Offline Wi-Fi Locks* on page 277, *Step 3: Syncing Doors with the SALTO Server* on page 286 and *Step 2: Syncing Doors with the Door Service Router* on page 296, respectively.

2. Click **Add Door**.
3. If door templates are used, the Templates dialog appears. To use the door settings from a template, which automatically fills in the fields on the Parameters and Operations tabs, select the template and click **OK**. Otherwise, click **Cancel**.

For Schlage IP-mode wireless devices or devices connecting to an RS485 hub, click **Cancel**.

4. Enter on the **Parameters** tab:

> **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| | |
|---|---|
| **Name** | Up to 50 characters for the name of the door. See *Appendix: pivCLASS Configuration* on page 503. |
| **Alt. Name** | An alternate name for the door. |
| **Location** | A short description of the door location. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | The panel that controls the door, the gateway that controls the IP-mode wireless device or the offline Wi-Fi device, or the external server that the ACM appliance is connected to. |
| | Displays for a panel that is connected to a subpanel that controls readers, locks, inputs and outputs; or a gateway that controls IP-mode wireless devices.<br>**Subpanel**: The name of the subpanel that is connected to the main panel or the name of the gateway.<br>**Door Number** or **Lock Number**: The door number for wired connections or lock number for wireless devices. For SimonsVoss wireless locks, use the hexadecimal address assigned by the SmartIntego Tool.<br>**Device Id**: Displays for Aperio AH-40 Hub subpanel only. The Lock/Sensor identifier from the Aperio programming application. |
| | Displays for a Schlage ENGAGE Gateway.<br>**Lock Model**: The lock model from the vendor.<br>**Linked Device**: The ID or name of each externally commissioned IP wireless or offline Wi-Fi device. For more information, refer to the commissioning process in vendor documentation. |
| | Displays for an ASSA ABLOY DSR.<br>**Lock Type**: The battery-powered or external-powered lock type from the vendor.<br>**Serial Number**: The serial number of the lock. |
| **Appliance** | The ACM appliance that is connected to the door, gateway, hub or external server. |
| **Vendor** | The manufacturer of the panel, gateway, offline Wi-Fi device or external server. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |

Displays for **Schlage** ENGAGE Gateway subpanel:

**Access Type**: Displays for an IP-connected wireless device only. Whether access is located on one or both sides of the door. Default is **Single**, which cannot be changed. For more information, see *Access Types* on page 204.

**Door Mode**: IP-connected wireless device only. The entry mode for the door when the gateway is online and communicating with the device. For information about the **Unlocked**, **Locked No Access** and **Card Only** options, see *Door Modes* on page 203.

*IP-connected RU exit device only (not applicable to RM).* The entry mode for the door when the gateway is online and communicating with the device. For more information about the **Unlocked** and **Locked No Access (Unlocked on Next Exit)** options, see *Door Modes* on page 203.

*Offline Wi-Fi lock only.* The entry mode for the door when the lock is online. For information about the **Card Only** option, see *Door Modes* on page 203.

**Lock Function**: None is the default (not applicable to RM device).

- **None**: Use the system default door settings.
- **Privacy**: When the interior lock button is pressed, the door will lock and the exterior lock will not grant access to any token. To unlock the door, the interior lock button must be pressed again or exit the room.

  **Note:** Only this lock function is supported for the ASSA ABLOY IP locks.

- **Apartment**: Use the interior lock button to toggle between locked and unlocked. When the door is locked, any valid token will open the door. The door must be manually locked or it will stay unlocked.
- **Classroom — Classroom/Storeroom** — The lockset is normally secure. The inside lever always allows free egress. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may be used to change to a passage or secured status. Not to be used on mortise deadbolt. Interior push button not to be used.

  **Note:** Only this lock function is supported for the RSI-connected NDE series lock.

  **Note:** This lock function is not supported for the IP-connected LE, LEB, NDE and NDEB series lock, or offline Wi-Fi lock.

- **Office** — The lockset is normally secure. The inside lever always allows free egress. An interior push-button on the inside housing may be used to select a passage or secured status. Meets the need for lockdown function for safety and security. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may also be used to change status. Not to

| | |
|---|---|
| | be used on mortise deadbolt.<br><br>**Note:** A Restore door action is available on the Door listing page and the Hardware Status page which resets the Door Mode to its default value.<br><br>**Always Mask Forced**: If selected, Door Forced Open alarms at the door are always masked.<br><br>**Always Mask Held**: If selected, Door Held Open alarms at the door are always masked.<br><br>**Custom Mode**: Another door mode that is supported by the gateway.<br><br>**Custom Schedule**: Displays for an IP-connected door (LE, LEB, NDE, NDEB series lock) if the Card Only door mode is selected, or IP-connected RU device if the Locked No Access door mode is selected. A predefined time when Custom Mode becomes active. **Never Active** is OFF. **24 Hours Active** is ON. |
| | For **Avigilon**, enter:<br><br>**Station Type**: Default is **ACM Verify** station, which is used on connected devices. A device that uses this station type of station is called an ACM Verify Station.<br><br>**Managed**: If selected, ACM Verify Station requires the user to grant or deny access to the person entering a valid PIN code. It also displays the name and picture of the user for verification.<br><br>**UnManaged**: If selected, ACM Verify Station automatically grants or denies access and does not provide additional information when a PIN code is entered.<br><br>**Geographic Timezone**: The time zone where the ACM Verify device is located if it is different from the time zone of the ACM appliance.<br><br>**Into Area**: The area that the badge holder enters by passing through the door and where the ACM Verify Station is used, or not, to monitor access to the area. You must specify an area if you want the virtual station to list all the people who have entered the area.<br><br>**Station Authentication**: The method of authentication on the ACM Verify device. **Login** specifies that the user log in to the ACM software using the ACM URL from the browser on the ACM Verify device. **Paired** specifies that the ACM Verify is paired to the ACM system. If the authentication type is Paired, the Door Add page refreshes and displays the Add Paired Device button.<br><br>**Tip:** The Avigilon settings do not require a panel. |

| | |
|---|---|
| | For **Mercury Security** and **HID** VertX panel, enter:<br>**Access Type**: Whether the reader is located on one or both sides of the door, or on an elevator door. See *Access Types* on page 204.<br>**Linked Door**: Displays for **Paired Primary** and **Paired Replica** access type only. The door with the reader on the other side of the door.<br>**Door Mode**: The entry mode of the door when the door controller is online and communicating with the panel. See *Door Modes* on page 203.<br>**Assurance Profile**: For Mercury Security LP4502 only. See *Appendix: pivCLASS Configuration* on page 503.<br>**Offline Door Mode**: The entry mode of the door if the door controller is no longer communicating with the panel.<br>**Note:** In many cases readers in offline mode require a very simple solution for entry or exit because of the memory limitations. The recommended Offline Door Mode option is **Locked No Access**.<br>**Custom Mode**: Another entry mode that is supported by the door module in addition to Door Mode and Offline Door Mode options.<br>**Custom Schedule**: When the Custom Mode becomes active. Never Active is OFF. 24 Hours Activeis ON.<br>**Masked Forced Schedule**: A predefined time when Door Forced Open alarms from the door will be masked.<br>**Masked Held Schedule**: A predefined time when Door Held Open alarms from the door will be masked.<br>**Always Mask Forced**: If selected, Door Forced Open alarms at the door are always masked.<br>**Always Mask Held**: If selected, Door Held Open alarms at the door are always masked. |
| | For **SALTO** panel, enter:<br>**Door Mode**: The entry mode of the door after syncing with the SALTO server and installing the door. See *Door Modes* on page 203.<br>**Custom Mode**: Another entry mode of the door that is time-based (see Custom Schedule). Can be **Unlocked**, **Card and Pin**, **Office**, **Toggle** or **Keypad Only**. If Keypad Only is selected, **Keypad Code** is displayed. You can enter up to 8 digits. See *Door Modes* on page 203.<br>**Custom Schedule**: A predefined time when Custom Mode becomes active.<br>**Always Mask Forced**: If selected, Door Forced Open alarms at the door are always masked.<br>**Always Mask Held**: If selected, Door Held Open alarms at the door are always masked. |

| | |
|---|---|
| **Door Processing Attributes** | For **Schlage** door, select:<br><br>**Note:** The following three attributes are not applicable to Control locks or offline Wi-Fi locks.<br><br>**Log Grants Right Away**: Initiates local I/O in the panel using the panel triggers. The system logs an extra event as soon as a grant occurs (that is, before entry / no entry is determined). This event is not turned into an Access Control Manager event.<br><br>Certain customers may have a trigger they want to fire (to execute a macro) as soon as there is a grant but before entry / no entry is determined.<br><br>**Log All Access as Used**: Logs all access grant transactions as if the person used the door. If this field is not selected, the door determines if it was opened and distinguishes if the door was used or not used for grant.<br><br>**Detailed Events**: Displays the current position of the door position switch (DPOS) in the Door State column of the door listing screen. When enabled the column displays “Open” when the DPOS is in an open state and “Closed” when the DPOS is in a closed state.<br><br>**Note:** To properly report the Door State from the Door Position Switch, Detailed Events must be enabled.<br><br>Typically, five to ten detailed transactions are generated for each grant transactions. During the normal course of operation, most guards don't need to see extensive reports on events; however, after hours, it is often useful to see every detail.<br><br>**Do Not Log Rex Transactions**: Indicates that request-to-exit transactions do not get logged to the database.<br><br>**Note:** This is the only attribute supported for offline Wi-Fi locks. |

For **Mercury Security** panel, select:

**Log Grants Right Away**: Initiates local I/O in the panel using the panel triggers. The system logs an extra event as soon as a grant ocurs (that is, before entry / no entry is determined). This event is not turned into an Access Control Manager event.

Certain customers may have a trigger they want to fire (to execute a macro) as soon as there is a grant but before entry / no entry is determined.

**Deny Duress** : Denies access to a user that indicates duress at a door.

**Don't Pulse Door Strike on REX**: Disables the pulse of the door strike output when the request-to-exit button is pressed and can be used for a 'quiet' exit. If not selected, the output is pulsed.

> **Note:** This field must not be checked for the SimonsVoss wireless lock, such as cylinders, on a door that does not support a door position switch (DPOS).

**Require Two Card Control**: Two tokens are required to open this door. This enforces the two-person rule at a specified door.

**Door Forced Filter:** : Filters door-forced alarms. Sometimes a door is either slow to close or is slammed shut and bounces open for a few seconds. With this filter, the monitor allows three seconds for a door to close before issuing an alarm.

**Log All Access as Used**: Logs all access grant transactions as if the person used the door.  If this field is not selected, the door determines if it was opened and distinguishes if the door was used or not used for grant.

**Detailed Events**: Displays the current position of the door position switch (DPOS) in the Door State column of the door listing screen. When enabled the column displays “Open” when the DPOS is in an open state and “Closed” when the DPOS is in a closed state.

> **Note:** To properly report the Door State from the Door Position Switch, Detailed Events must be enabled.

Typically, five to ten detailed transactions are generated for each grant transactions. During the normal course of operation, most guards don't need to see extensive reports on events; however, after hours, it is often useful to see every detail.

**Enable Cipher Mode**: Enables the operator to enter card number digits at the door’s keypad.

**Use Shunt Relay**:Enables the use of a shunt relay for this door.

**Do Not Log Rex Transactions**: Indicates that request-to-exit transactions do not get logged to the database.

| | |
|---|---|
| | For **HID** VertX panel, select:<br>**Door use Tracking**: The level of door event tracking that is logged in the Monitor screen. These options should only be used when the **Detailed Events** option is enabled.<br>• **None**: Only standard door events are logged.<br>• **Used**: The details of when the door is used.<br>• **Used with pending**: The events that occur between door use.<br>**Deny Duress**: If selected, denies access to a user who is in duress at a door.<br>**Don't Pulse Door Strike on REX**: Disables the pulse of the door strike when request-to-exit button is activated.<br>**Detailed Events**: For circumstances when it is important to know all the details of an event. Displays the current position of the door position switch (DPOS) in the Door State column of the Door list. When enabled the column displays “Open” when the DPOS is in an open state and “Closed” when the DPOS is in a closed state.<br>**Enable Cipher Mode**: Allows the operator to enter card number digits at the door’s keypad.<br>**Do Not Log Rex Transactions**: Disables logging of request-to-exit transactions. |
| | For **SALTO** panel, select:<br>**Detailed events**: Enables the reporting of event details, such as Door State and Door Mode, after syncing and installing the door.<br>**Do Not Log Rex Transactions**: Disables logging of request-to-exit transactions. |

5. Click ✔ to add the door. Once saved the page becomes the Door: Edit page. If a door template was used, the fields on the Parameters and Operations tabs are entered.
6. To edit door configuration, see *Editing Doors* on page 201. To edit lock configuration, see *Step 3: Configuring IP-enabled Wireless Devices* on page 269.
   - **Parameters**: Edit access type, processing attributes, lock functions, and other options.
   - **Operations**: Displays for HID VertX, Mercury Security, Schlage wired and RSI wireless locks, and ASSA ABLOY IP locks only. Edit simple macros, accepted card formats and other options.
   - **Hardware**: Displays for HID VertX, Mercury Security, and Schlage wired and RSI wireless locks only. Edit reader, door position, strike and request to exit (REX).
   - **Elev**: Displays for Mercury Security only. View elevator door details.
   - **Cameras**: Add or remove associated cameras.
   - **Interlocks**: Displays for Mercury Security only. Sets interlocks.
   - **Events**: View and edit door events.
   - **Access**: Does not display for RU and RM exit devices. View access groups, roles and identities that have door access.
   - **Transactions**: View door transactions.
   - **Notes**: Add notes about the door and review previous notes, if any.
7. Click ✔ to save your changes.

***Doors - VertX® New Parameters page***

After you save a new door for the first time, the screen refreshes and displays the initial Parameters page for the door.

| Feature | Description |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | Specify the panel the door is assigned to.<br><br>After you make your selection, new options may be displayed to define how the door is connected to the panel. |
| **Subpanel** | Specify the subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the specified panel. |
| **Lock Number** | Specifies a configured group of readers, inputs, and outputs that are connected from the subpanel to the door. Select the lock number from the drop-down list. |
| **Access Type** | Select the Access Type for the door.<br><br>**Tip:** If the access type is a paired door (paired primary or paired replica), the Door Add page re-displays with the additional field, Paired Door. Select the Paired Door option from the drop down list. |
| **Door Mode** | Select the entry mode for the door when the door controller is online and communicating with the panel. |
| **Offline Door Mode** | Select the entry mode used for the door if the door controller is no longer communicating with the panel.<br><br>**Note:** In many cases readers in offline mode require a very simple solution for entry or exit because of the memory limitations. The recommended Offline Door Mode option is **Locked No Access**. |
| **Custom Mode** | Select any additional door mode the door must support outside the Door Mode and Offline Mode options. |
| **Custom Schedule** | Define when the Custom Mode would be active.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Mask Forced Schedule** | Define when Door Forced Open alarms from this door will be masked.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |

| Feature | Description |
|---|---|
| **Mask Held Schedule** | Define when Door Held Open alarms from this door will be masked.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Always Mask Forced** | Check this box to mask all Forced Door events. |
| **Always Mask Held** | Check this box to mask all Door Held Open events. |
| **Door Processing Attributes** | |
| **Door use Tracking** | Select one of the listed options to define the level of door event tracking that is logged in the Monitor screen.<br><br>• **None**: only standard door events are logged<br>• **Used**: includes the details of when the door is used<br>• **Used with pending**: includes the events that occur between door use.<br><br>These options should only be used when the **Detailed events** option is enabled. |
| **Deny Duress** | If a user indicates duress at a door, checking this box denies access. |
| **Don't Pulse Door Strike on REX** | Check this box to disable the pulse of the door strike when request-to-exit button is activated. |
| **Detailed Events** | Check this box to generate detailed events of all hardware at the door including door position masking, timer expiration and output status.<br><br>This feature is useful for circumstances where it is important to know all the details of an event. |
| **Enable Cipher Mode** | Check this box to enable cipher mode.<br><br>Cipher mode allows the operator to enter card number digits at the door's keypad. |
| **Do Not Log Rex Transactions** | Check this box to disable logging of request-to-exit transactions. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

***Doors - Mercury Security New Parameters page***

After you save a new door for the first time, the screen refreshes and displays the initial Parameters page for the door.

> **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| Feature | Description |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |

| Feature | Description |
|---|---|
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | Specifies the panel the door is assigned to.<br><br>After you make your selection, new options may be displayed to define how the door is connected to the panel. |
| **Subpanel** | Specifies the subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the selected main panel. |
| **Door Number** | A configured group of readers, inputs, and outputs that are connected from the subpanel to the door.<br><br>For wired connections, the door number from the drop-down list.<br><br>For wireless locks only:<br><br>• The number programmed for the lock. For all locks except SimonsVoss, select the number from the drop-down list.<br>• For SimonsVoss wireless locks, the hexadecimal address assigned by the SmartIntego Tool. For more information, see *Configuring SimonsVoss Wireless Locks* on page 183. |
| **Access Type** | Select the Access Type from the drop down list.<br><br>**Tip:** If the access type is a paired door (paired primary or paired replica), the Door Add page re-displays with the additional field, Paired Door. Select the Paired Door option from the drop down list. |
| **Door mode** | The entry mode for the door when the door controller is online and communicating with the panel.<br><br>Select a Door Mode option from the drop down list. |
| **Offline Door Mode** | The entry mode used for the door if the door controller is no longer communicating with the panel.<br><br>**Note:** In many cases readers in offline mode require a very simple solution for entry or exit because of the memory limitations. The recommended Offline Door Mode option is **Locked No Access**.<br><br>Select the Offline Mode option from the drop down list. |

| Feature | Description |
|---|---|
| **Lock Function** | Select how the interior lock button will function.<br>• **Privacy** — When you press the interior lock button, the door will lock and the exterior lock will not grant access to any token. To unlock, you must press the interior lock button again or exit the room.<br>• **Apartment** — When you press the interior lock button, the door will lock but any valid token will open the door. The door must be manually locked or it will stay unlocked.<br>• **Classroom** — Classroom/Storeroom. The lockset is normally secure. The inside lever always allows free egress. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may be used to change to a passage or secured status. Not to be used on mortise deadbolt. Interior push button not to be used.<br>• **Office** — The lockset is normally secure. The inside lever always allows free egress. An interior push-button on the inside housing may be used to select a passage or secured status. Meets the need for lockdown function for safety and security. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may also be used to change status. Not to be used on mortise deadbolt.<br>There is a Restore door action available on the Hardware Status page or Door Listing page which resets the door's configuration values to their default value. If the door is in any mode (Classroom, Office, Privacy, or Apartment) it will be 'restored' to the opposite status (e.g. if the door is in Privacy mode then it is locked - if the Restore option is selected then the door will return to its default mode, which is the mode set in the base configuration for the door). |
| **Custom Mode** | Select any additional door mode the door must support outside the Door Mode and Offline Mode options. |
| **Custom Schedule** | Define when the Custom Mode would be active.<br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Mask Forced Schedule** | Define when Door Forced Open alarms from this door will be masked.<br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Mask Held Schedule** | Define when Door Held Open alarms from this door will be masked.<br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Always Mask Forced** | Check this box to specify that Door Forced Open alarms at this door are always masked.<br>Normally, this box is unchecked. |
| **Always Mask Held** | Check this box to specify that Door Held Open alarms at this door are always masked.<br>Normally, this box is unchecked. |
| **Door Processing Attributes** | |
| **Log grants right away** | When this box is checked, the system logs an extra event as soon as there is a grant (that is, before entry / no entry is determined). This event is not turned into a Access Control Manager event. Check this box in order to initiate local I/O in the panel using the panel triggers.<br>Certain customers may have a trigger they want to fire (to execute a macro) as soon as there is a grant but before entry / no entry is determined. |
| **Deny duress** | Check this box to deny access to a user that indicates duress at a door. |

| Feature | Description |
|---|---|
| **Don't pulse door strike on REX** | Check this box to disable the pulse of the door strike output when the request-to-exit button is pressed and can be used for a 'quiet' exit.<br><br>If this box is not checked, the output is pulsed.<br><br>For SimonsVoss wireless lock doors that do not support a door position switch (DPOS) , this box must not be checked. |
| **Require two card control** | Check this box to specify that two tokens are required to open this door. This enforces two-person rule at a specified door. |
| **Door Forced Filter** | Check this box to enable the filter feature for door forced alarms.<br><br>There are instances when a door is either slow to close or is slammed shut and bounces open for a few seconds. With this filter, the monitor allows three seconds for a door to close before issuing an alarm. |
| **Log all access as used** | Check this box to log all access grant transactions as if the person used the door. If this box is not checked, the door determines if it was opened and will distinguish if the door was used or not used for grant. |
| **Detailed events** | Check this box to display the current position of the door position switch (DPOS) in the Door State column of the door listing screen. When enabled the column will display “Open” when the DPOS is in an open state and “Closed” when the DPOS is in a closed state.<br><br>**Note:** To properly report the Door State from the Door Position Switch, Detailed Events must be enabled.<br><br>Typically, five to ten detailed transactions will be generated for each grant transactions. During the normal course of operation, most guards don't need to see extensive reports on events; however, after hours, it is often useful to see every detail. |
| **Enable cipher mode** | Check this box to enable cipher mode.<br><br>Cipher mode allows the operator to enter card number digits at the door’s keypad. |
| **Use Shunt Relay** | Check this box to enable the use of a shunt relay for this door. |
| **Do Not Log Rex Transactions** | Check this box to indicate that return-to-exit transactions do not get logged to the database. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## Doors - Door: Edit Screen

When you click the name of an existing door from the Doors list, the Door: Edit screen is displayed.

For definitions of the relevant fields and pages for each door type, refer to the page specific to your door vendor.


- *Door: Edit page (VertX®)* on the next page
- *Door: Edit page (Mercury Security)* on page 239

### *Door: Edit page (VertX® )*

When you select a VertX® door, the configurable options are arranged in tabs on the Door: Edit page.

#### Parameters tab (VertX® )

Define the door connections, door mode, schedule and processing attributes on the **Parameters** tab on the Door Edit page.

| | |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | The panel the door is assigned to.<br><br>After you make your selection, new options may be displayed to define how the door is connected to the panel. |
| **Subpanel** | The subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the specified panel. |
| **Lock Number** | A configured group of readers, inputs, and outputs that are connected from the subpanel to the door. Select the lock number from the drop-down list. |
| **Access Type** | The Access Type for the door.<br><br>**Tip:** If the access type is a paired door (paired primary or paired replica), the Door Add page re-displays with the additional field, Paired Door. Select the Paired Door option from the drop down list. |
| **Door Mode** | The entry mode for the door when the door controller is online and communicating with the panel. |
| **Offline Door Mode** | The entry mode used for the door if the door controller is no longer communicating with the panel. The Offline Door Mode is no longer supported if the door controller is connected to an LP4502 panel that has replaced an HID VertX panel.<br><br>**Note:** In many cases readers in offline mode require a very simple solution for entry or exit because of the memory limitations. The recommended Offline Door Mode option is **Locked No Access**. |
| **Custom Mode** | Any additional door mode the door must support outside the Door Mode and Offline Mode options. |

| | |
|---|---|
| **Custom Schedule** | When the Custom Mode would be active.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Mask Forced Schedule** | When Door Forced Open alarms from this door will be masked.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Mask Held Schedule** | When Door Held Open alarms from this door will be masked.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Always Mask Forced** | Check this box to mask all Forced Door events. |
| **Always Mask Held** | Check this box to mask all Door Held Open events. |
| **Door Processing Attributes** | |
| **Door use Tracking** | The level of door event tracking that is logged in the Monitor page.<br><br>• **None**: Only standard door events are logged.<br>• **Used**: Includes the details of when the door is used.<br>• **Used with pending**: Includes the events that occur between door use.<br><br>These options should only be used when the **Detailed events** option is enabled.<br><br>**Note:** The Door use Tracking door processing attribute is not used, if the door is connected to a Mercury Security LP4502 panel that has replaced an HID VertX panel. |
| **Deny Duress** | If a user indicates duress at a door, checking this box denies access. |
| **Don't Pulse Door Strike on REX** | Check this box to disable the pulse of the door strike when request-to-exit button is activated. |
| **Detailed Events** | Check this box to generate detailed events of all hardware at the door including door position masking, timer expiration and output status.<br><br>This feature is useful for circumstances where it is important to know all the details of an event. |
| **Enable Cipher Mode** | Check this box to enable cipher mode.<br><br>Cipher mode allows the operator to enter card number digits at the door's keypad. |
| **Do Not Log Rex Transactions** | Check this box to disable logging of request-to-exit transactions. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

| | |
|---|---|
| **Create New Report** | Click this button to generate a PDF report on this door. |
| **Add Door** | Click this button to add a new door. |
| **Transaction Report** | Click this button to generate a PDF transaction report on this door. |
| **Show Policy** | Click this button to generate a PDF report on the current door policy. |
| | Click this button to delete this door.<br><br>Click **OK** in the dialog box that displays to confirm the deletion. The door will be deleted and you will be returned to the Doors list. |

### Operations tab (VertX®)

Edit door operations, including the door mode, door held pre-alarms, anti-passback and strike modes.

| | |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | The panel the door is assigned to. |
| **Subpanel** | The subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the selected main panel. |
| **Lock Number** | The number ID for the set of inputs/outputs that are connected from the subpanel to the door.<br><br>This option is only displayed if there are inputs or outputs connected to the selected subpanel. |
| **APB Mode** | The anti-passback mode for the door.<br><br>For a description of each option, see *Anti-Passback Modes* on page 205. |
| **APB Delay** | The number of seconds before another entry is allowed.<br><br>Enter the number of seconds. |
| **Into Area** | The area the user enters when passing through the door. If no area is specified, any location is valid.<br><br>Select the area from the drop down list. Only those areas currently defined for this system appear in this list. |
| **Out of area** | The area the user moves into when exiting the door.<br><br>Select the area from the drop down list. |

| | |
|---|---|
| **Strike Mode** | When a door should unlock. Specifies if the strike is deactivated when the door is opened, when the door is closed, or when the strike timer expires.<br><br>Select the strike mode from the drop down list.<br><br>• **Cut short when open** — When the Minimum Strike Time is set to 0 the strike is deactivated when the door opens or after the duration specified in Standard Access Time. Otherwise, the strike is deactiveated after the duration specified in the Minimum Strike Time. This option requires that the door has a door position switch (DPOS) installed to monitor the Open and Closed door states.<br>• **Turn off on close** — The strike is deactivated when the door closes. This option requires that the door has a DPOS installed to monitor the Open and Closed door states. Time settings of Minimum Strike Time and Standard Access Time are irrelevant.<br>• **Full strike time** — The strike is deactivated when the strike timer expires. This strike mode is directly related to the time setting for Standard Access Time. |
| **Held Pre-Alarm** | The number of seconds a door can be held open before a pre-alarm is issued. If activated, the 'Door held open pre-alarm' event may be used to send an email notification.<br><br>Example: `20` seconds<br><br>If `120` seconds is entered in Held Open Time, the pre-alarm warning will be sent at 100 seconds and the 'Door held open' event at 120 seconds.<br><br>If `200` seconds is entered in Extended Held Open Time, the pre-alarm warning will be sent at 180 seconds and the 'Door held open' event at 200 seconds.<br><br>For more information, see *Configuring Door Held-Open Settings* on page 192. |
| **Minimum Strike Time** | The minimum amount of time the door will be unlocked. Each time the door is unlocked and open, the door will remain unlocked for the set amount of time. If you hold the door open for longer than the set amount of time, the door automatically re-locks when it closes.<br><br>Enter the number of seconds. Default setting is 0 seconds.<br><br>If the value is set to 0, the door will remain unlocked for the amount of time set for the Standard Access Time.<br><br>This setting only applies when the Strike Mode is set to Cut short when open. |
| **Standard Access Time** | The number of seconds the door remains unlocked after access has been granted.<br><br>If the door is not opened within this time, it will automatically lock.<br><br>This setting only applies and must be configured when the Strike Mode is set to Cut short when open or Full strike time. |
| **Held Open Time** | The number of seconds a door can be held open before a 'Door held open' event is generated.<br><br>Example: `120` seconds<br><br>For more information, see *Configuring Door Held-Open Settings* on page 192. |
| **Extended Access** | The strike time for a door configured for persons that require more time to enter through a door.<br><br>Enter the number of seconds. |

| | |
|---|---|
| **Extended Held Open Time** | The number of seconds a door can be held open for users with extended access permissions before a Door held open' event is generated.<br><br>This feature is useful for users that may require more time to enter a door, such as individuals with accessibility needs.<br><br>Example: 200 seconds<br><br>For more information, see *Configuring Door Held-Open Settings* on page 192. |
| **Card Formats** | The card formats that are compatible with the reader at the door.<br><br>Check the box beside the card formats that apply. |
| **Simple Macros** | |
| **Type** | A default macro that is triggered when the following conditions are met for this door. Currently available macros include:<br><br>• Forced<br>• Held<br>• Pre-Alarm |
| **Schedule** | Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Output** | An output that is activated by the Type condition. |
| **Commands** | Click **Save Macro** to save the settings for this canned macro. If this is a new macro, a new row is automatically added below.<br><br>Click **Remove Macro** to delete a macro. This button only appears if the macro has been saved in the system.<br><br>For more information, see *Adding Simple Macros* on page 200. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Create New Report** | Click this button to generate a PDF report on this door. |
| **Add Door** | Click this button to add a new door to the system. |
| **Transaction Report** | Click this button to generate a PDF transaction report on this door. |
| **Show Policy** | Click this button to generate a PDF report on the current door policy. |

### Hardware tab (VertX®)

When you click the **Hardware** tab at the Door Edit screen, the HID Hardware page is displayed. This page allows you to connect and edit readers, inputs and outputs to the door.

| Feature | Description |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |

| Feature | Description |
|---|---|
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | Specifies the panel the door is assigned to. |
| **Subpanel** | Specifies the subpanel that is connected to the door.<br>This option is only displayed if there is a subpanel connected to the selected main panel. |
| **Lock Number** | The number ID for the set of inputs/outputs that are connected from the subpanel to the door.<br>This option is only displayed if there are inputs or outputs connected to the selected subpanel. |
| | To edit one of the readers, inputs or outputs that are connected to the door, click beside the hardware item:<br>• If you click beside the Reader or Alternate Reader, the Reader Edit page is displayed.<br>• If you click beside the Door Position, REX #1 or Rex#2, the Input Edit page is displayed.<br>• If you click beside Strike, the Output Edit page is displayed. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Create New Report** | Click this button to generate a PDF report on this door. |
| **Add New Door** | Click this button to add a new door to the system. |
| **Transaction Report** | Click this button to generate a PDF transaction report on this door. |
| **Show Policy** | Click this button to generate a PDF report on the current door policy. |

# Reader Edit page (VertX®)

When you click the icon beside the Reader or Alternate Reader field on the Door Hardware page, the Reader Edit page is displayed. This page allows you to define the options for this reader.

| Feature | Description |
|---|---|
| **Name** | Enter the name of this reader. |
| **Alt. name** | Enter an alternative name for this reader. |
| **Location** | Enter a brief description of the location of this reader. |

| Feature | Description |
|---|---|
| **Keypad decode** | From the drop down option list, select the keypad decode or enryption method you want to use for this reader. Choose from these options:<br>• **Hughes ID 4-bit**<br>• **Indala**<br>• **MR20 8-bit no tamper** |
| **Wiegand** | Check this box to indicate that this reader supports the Wiegand standard. |
| **NCI magstripe** | Check this box to indicate that this reader supports the NCI magstripe standard. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

# Input Edit page (VertX®)

When you click the icon beside the Door Position or REX # field on the Door Hardware page, the Input Edit page is displayed. This page allows you to define the options for this input.

| Feature | Description |
|---|---|
| **Input** | The name of the input point. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Address** | The read-only address of this point. |
| **Supervision** | If resistors are used to monitor the input, select the level of resistance expected to indicate open or closed.<br>**Note:** This setting is not supported for HID VertX V100 inputs that are wired to Mercury Security LP4502 panels. |
| **Debounce**[1] | From the drop down list, select the number of units this input should be allowed to debounce. The units are listed in milliseconds (ms). |
| **Cameras** | Select the camera from the window that this input activates if it goes into alarm.<br>Only the cameras that have been added to the system are listed. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |

[1]Due to mechanical properties of a switch, when a switch is closed, there is a period of time in which the electrical connection "bounces" between open and closed. To a microcontroller, this "bouncing" can be interpreted as multiple button pushes. To suppress the "bouncing", the controller software is designed to anticipate it. This is known as "debouncing a switch".

| Feature | Description |
|---|---|
| | Click this button to discard your changes. |
| **Show Policy** | Click this button to display the policies associated with this input module. |

# Output Edit page (VertX®)

When you click the icon beside the Strike field on the Door Hardware page, the Output Edit page is displayed. This page allows you to define the options for this output.

**Note:** VertX® output panels do not have an operating mode option because they are automatically energized when active. You can set the panels to be "not energized when active" if wired in reverse.

| Feature | Description |
|---|---|
| **Output** | The name of this output point. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Address** | The read-only address for this output point. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Show Policy** | Click this button to display the policies associated with this output module. |

### Cameras tab (VertX®)

When you click the **Cameras** tab on the Door Edit screen, the HID Camera page is displayed. From this page, you can assign specific cameras to record video of the selected door.

| Feature | Description |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |

| Feature | Description |
|---|---|
| **Panel** | Specifies the panel the door is assigned to.<br><br>After you make your selection, new options may be displayed to define how the door is connected to the panel.<br><br>Not applicable to Avigilon doors. |
| **Subpanel** | Specifies the subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the selected main panel.<br><br>Not applicable to Avigilon doors. |
| **Lock Number** | Enter the number ID for the set of inputs/outputs that are connected from the subpanel to the door.<br><br>This option is only displayed if there are inputs or outputs connected to the selected subpanel. |
| **Door Number** | The number that has been assigned to the door module by the wireless lock configuration device. |
| **Camera Type** | Select the external system that is connected to the camera.<br><br>The Available window is populated with those cameras that fit this definition.<br><br>Click the **Camera** button beside this field to view live video from the camera. For more information on the video viewer window, see *Configuring and Viewing Live Video Stream* on page 253. |
| **Available** | This window displays a list of cameras that have been configured in the system.<br><br>To connect a camera to the door, select the camera from the Available list, then click ► to move it to the Members list. |
| **Members** | The window displays a list of cameras that are currently connected to the door.<br><br>To disconnect a camera from the door, select the camera from the Members list, then click ◄ to move it to the Available list. |
| **Search** | If you have more than 10 cameras, the Search feature may be displayed to help you find the cameras you need.<br><br>In the **Search** field, enter the name of the camera you want to find, then click **Filter**. You can narrow your search by selecting the **Case-sensitive** option. Click **Clear** to restore the full list of available cameras. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |
| | Click this button to generate a PDF report on this door. |
| **Add Door** | Click this button to add a new door. |
| **Transaction Report** | Click this button to generate a PDF transaction report on this door. |
| **Show Policy** | Click this link to view a PDF report indicating the current policy associated with this door. |

## Events tab

For Mercury Security, VertX and Avigilon doors

View door events on the **Events** tab in **Physical Access**.

This page lists all the local and global events that can be triggered by this door. The Local Events table is only listed when there are local events configured for the door.

**Local Events**

This table is only displayed if there are local events for the device.

| | |
|---|---|
| **Name** | The name of this event.<br><br>Click the name to edit the local event. |
| **Event** | The event type. |
| **Source Type** | The source of this event. |
| **Has On/Off** | If the event toggles on or off.<br><br>Click **Yes** or **No**. |
| **Masked** | If the event is masked.<br><br>Click to change status to (yes) or (no). |
| **Logged** | If the event is logged.<br><br>Click to change status to (yes) or (no). |
| **Show Video** | If a video is available for the event. If 'yes' is selected, the live video window automatically pops up when the event is received.<br><br>Click to change status to (yes) or (no). |
| | Click this button to delete the local event. |

**Global Events**

This table displays all the global events that are related to this type of device.

| | |
|---|---|
| **Name** | The name of this event. |
| **Event** | The event type. |
| **Source Type** | the source of this event. |
| **Has On/Off** | If the event toggles on or off.<br><br>Click **Yes** or **No**. |
| **Masked** | If the event is masked.<br><br>Click to change status to (yes) or (no). |
| **Logged** | If the event is logged.<br><br>Click to change status to (yes) or (no). |
| **Show Video** | If a video is available for the event. If 'yes' is selected, the live video window automatically pops up when the event is received.<br><br>Click to change status to (yes) or (no). |

| | |
|---|---|
| **Create Local** | Click this button to create a version of this global event that only applies to the specific device. |

# Doors - Creating Local Events for VertX® Doors

When you click the **Create Local** button from the Door Events page, the local version of the Event page is displayed. This page is a copy of the global event that can be customized as a local event for this specific door.

> **Note:** Changes on this page do not affect the global event.

Make any changes as required.

| Feature | Description |
|---|---|
| **Name** | The name of the event, which you can change if the name is not. |
| **Return Name** | The name used to identify that this event is over, or the return-to-normal (RTN) ) name of this event, such as the door closing and locking after access has been granted, or after the configured door open time has expired. |
| **Event Type** | The event type.<br><br>Only events types that have been defined in the system appear in the drop down list. |
| **Source Type** | The device that is the source of the event. |
| **Priority** | The priority of this event.<br><br>The priority range is 1 - 999.<br><br>The Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. |
| **Alarm Sound** | A sound that is played when a new alarm occurs while you are monitoring the Alarms page.<br><br>**Note:** A default beeping sound is played, if no sound is selected. |
| **Suppress Time** | A schedule when alarm events are not reported.<br><br>Only schedules that have been defined in the system are listed. |
| **Instructions** | Any instructions that may be required for handling this event.<br><br>The instructions are made available to the user on the Monitor screen. |
| **Return Event** | The event type of the RTN event. |
| **Return Priority** | The priority of the RTN event.<br><br>The priority range is 1 - 999. |

| Feature | Description |
|---|---|
| **Has on/off** | This event has an RTN event associated with it.<br><br>**Note:** Adding return event information manually on this screen does not change the setting of this checkbox. It is set only if the original event has an associated RTN event defined for it. |
| **Masked** | This box indicates that this a masked event by default. This can be changed on the Event List page. |
| **Logged** | This box indicates to log the event by default. This can be changed on the Event List page.<br><br>Note that if Event Type logging is turned on, then all Events of that Event Type are logged, regardless of their individual logging configuration. If Event Type logging is turned off, then the logging configuration of the specific Events of that Event type are adhered to. |
| **Show Video** | This box indicates to auto-launch video from the linked camera feed when the event occurs by default. This can be changed on the Event List page.<br><br>This feature only works if video is enabled. |
| **Two Person Required To Clear** | This box indicates that two people are required to acknowledge and clear this event.<br><br>If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge.<br><br>If the same operator attempts to clear the alarm, then nothing will happen. |
| **Email** | The email address of all the people who should be notified when this event occurs.<br><br>You can enter more than one email address separated by a comma. |
| **Roles:** | |
| **Available** | A list of all the roles that are available to you in the system.<br><br>To allow specific role to have access to view or edit this event, select a role from the Available list then click ▶ to add the role to the Member list.<br><br>To move one or more roles to the Members window, click to select one role then **Ctrl** + click to select a non-consecutive group of roles, or **Shift** + click to select a consecutive roles. |
| **Members** | A list of all the roles that are able to view or edit this event.<br><br>If this event is associated with at least one role, then any user who does not have the selected roles will not be able to view or edit the event. |

### Access tab (VertX® )

When you click the **Access** tab on the Door: Edit screen, the Access page is displayed. This page provides a list of the access groups, roles and identities that have permission to edit or use this door.

| Feature | Description |
|---|---|
| **Access Group** | The name of this access group. Click this link to edit the access group. |
| **Roles** | Lists the roles this access group is a member of.<br><br>Click the **+** or **-** symbol beside each role to show or hide the identities that are in the access group through the role. |

| Feature | Description |
|---|---|
| **Identities** | Lists the users who are members of the access group. |

### Transactions tab (VertX® )

When you click the **Transactions** tab on the Door: Edit screen, the HID Transaction page is displayed.

This page allows you to review events and alarms that have occurred at this door. The table displays the following information about each event:

| Feature | Description |
|---|---|
| **Panel Date** | The date and time when the event occurred. |
| **Priority** | The priority of the event. The highest priority is 1 and the lowest priority is 999. |
| **Event** | The name of the event. |
| **Last Name** | The last name of the person who generated the event. |
| **First Name** | The first name of the person who generated the event. |
| **Card Number** | The internal token number assigned to the person who generated the event. |
| **Message** | This displays any messages that may be associated with the event. |

## *Door: Edit page (Mercury Security)*

When you select a Mercury Security door, the configurable options are arranged in tabs on the Door: Edit page.

### Parameters tab (Mercury Security)

When you click the **Parameters** tab on the Door Edit screen, the Parameters page is displayed. This page allows you to define the door connections, door mode, schedule and processing attributes.

> **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| Feature | Description |
|---|---|
| **Name** | The name of the door.<br><br>See *Appendix: pivCLASS Configuration* on page 503. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |

| Feature | Description |
|---|---|
| **Panel** | Specifies the panel the door is assigned to.<br><br>After you make your selection, new options may be displayed to define how the door is connected to the panel. |
| **Subpanel** | Specifies the subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the selected main panel. |
| **Lock Number or Door Number** | A configured group of readers, inputs, and outputs that are connected from the subpanel to the door.<br><br>For wired connections, the door number from the drop-down list.<br><br>For wireless locks only:<br><br>• The number programmed for the lock. For all locks except SimonsVoss, select the number from the drop-down list.<br>• For SimonsVoss wireless locks, the hexadecimal address assigned by the SmartIntego Tool. For more information, see *Configuring SimonsVoss Wireless Locks* on page 183. |
| **Access Type** | Select the Access Type from the drop down list. Any door that is created with this template will be set to this type.<br><br>Use Single for a door with one reader on one side of the door only (single reader door). Use Paired Primary and Paired Replica for a door with two readers, one on each side of the door (paired reader door). Paired readers allow each side of a single physical door to act like a separate door. This is particularly useful for anti-passback and mustering.<br><br>If you set the access type to either Paired Primary or Paired Replica, when you add a door using this template, the Door Add page displays with the additional field, Linked Door. Use this field to select the door with the reader on the other side. The linking between the doors has to be done separately from adding the door.<br><br>The Access Type can also be configured in the Wiring Template. When configured in both the Wiring Template, and the associated Door Template, the setting in the Wiring Template takes precedence. It is recommended that you use the Wiring Template to efficiently create linked paired doors. |
| **Door Mode** | The entry mode for the door when the door controller is online and communicating with the panel.<br><br>Select a Door Mode option from the drop down list. |
| **Offline Mode** | The entry mode used for the door if the door controller is no longer communicating with the panel. The Offline Door Mode is no longer supported if the door controller is connected to an LP4502 panel that has replaced an HID VertX panel.<br><br>**Note:** In many cases readers in offline mode require a very simple solution for entry or exit because of the memory limitations. The recommended Offline Door Mode option is **Locked No Access**.<br><br>Select the Offline Mode option from the drop down list. |

| Feature | Description |
|---|---|
| **Lock Function** | Select how the interior lock button will function.<br>• **Privacy** — When you press the interior lock button, the door will lock and the exterior lock will not grant access to any token. To unlock, you must press the interior lock button again or exit the room.<br>• **Apartment** — When you press the interior lock button, the door will lock but any valid token will open the door. The door must be manually locked or it will stay unlocked.<br>• **Classroom** — Classroom/Storeroom. The lockset is normally secure. The inside lever always allows free egress. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may be used to change to a passage or secured status. Not to be used on mortise deadbolt. Interior push button not to be used.<br>• **Office** — The lockset is normally secure. The inside lever always allows free egress. An interior push-button on the inside housing may be used to select a passage or secured status. Meets the need for lockdown function for safety and security. Valid toggle credentials (i.e. a valid card that is swiped twice within five seconds) on the exterior may also be used to change status. Not to be used on mortise deadbolt.<br>There is a Restore door action available on the Hardware Status page or Door Listing page which resets the door's configuration values to their default value. If the door is in any mode (Classroom, Office, Privacy, or Apartment) it will be 'restored' to the opposite status (e.g. if the door is in Privacy mode then it is locked - if the Restore option is selected then the door will return to its default mode, which is the mode set in the base configuration for the door). |
| **Custom Mode** | Select any additional door mode the door must support outside the Door Mode and Offline Mode options. |
| **Custom Schedule** | Define when the Custom Mode would be active.<br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Mask Forced Schedule** | Define when Door Forced Open alarms from this door will be masked.<br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Mask Held Schedule** | Define when Door Held Open alarms from this door will be masked.<br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Always Mask Forced** | Check this box to specify that Door Forced Open alarms at this door are always masked.<br>Normally, this box is unchecked. |
| **Always Mask Held** | Check this box to specify that Door Held Open alarms at this door are always masked.<br>Normally, this box is unchecked. |
| **Door Processing Attributes** | |
| **Log Grants Right Away** | When this box is checked, the system logs an extra event as soon as there is a grant (that is, before entry / no entry is determined). This event is not turned into a Access Control Manager event. Check this box in order to initiate local I/O in the panel using the panel triggers.<br>Certain customers may have a trigger they want to fire (to execute a macro) as soon as there is a grant but before entry / no entry is determined. |
| **Deny Duress** | Check this box to deny access to a user that indicates duress at a door. |

| Feature | Description |
|---|---|
| **Don't Pulse Door Strike on REX** | Check this box to disable the pulse of the door strike output when the request-to-exit button is pressed and can be used for a 'quiet' exit.<br><br>If this box is not checked, the output is pulsed. |
| **Require Two Card Control** | Check this box to specify that two tokens are required to open this door. This enforces two-person rule at a specified door. |
| **Door Forced Filter** | Check this box to enable the filter feature for door forced alarms.<br><br>There are instances when a door is either slow to close or is slammed shut and bounces open for a few seconds. With this filter, the monitor allows three seconds for a door to close before issuing an alarm. |
| **Log All Access as Used** | Check this box to log all access grant transactions as if the person used the door. If this box is not checked, the door determines if it was opened and will distinguish if the door was used or not used for grant. |
| **Detailed Events** | Check this box to display the current position of the door position switch (DPOS) in the Door State column of the door listing screen. When enabled the column will display “Open” when the DPOS is in an open state and “Closed” when the DPOS is in a closed state.<br><br>**Note:** To properly report the Door State from the Door Position Switch, Detailed Events must be enabled.<br><br>Typically, five to ten detailed transactions will be generated for each grant transactions. During the normal course of operation, most guards don't need to see extensive reports on events; however, after hours, it is often useful to see every detail. |
| **Enable Cipher Mode** | Check this box to enable cipher mode.<br><br>Cipher mode allows the operator to enter card number digits at the door’s keypad. |
| **Use Shunt Relay** | Check this box to enable the use of a shunt relay for this door. |
| **Do Not Log Rex Transactions** | Check this box to indicate that return-to-exit transactions do not get logged to the database. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Create New Report** | Click this button to generate a PDF report on this door. |
| **Add Door** | Click this button to add a new door. |
| **Transaction Report** | Click this button to generate a PDF transaction report on this door. |
| **Show Policy** | Click this button to generate a PDF report on the current door policy. |
| | Click this button to delete this door.<br><br>Click **OK** in the dialog box that displays to confirm the deletion. The door will be deleted and you will be returned to the Doors list. |

### Operations tab (Mercury Security)

Edit door operations, including the door mode, door held pre-alarms, anti-passback and strike modes.

> **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| | |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | The panel the door is assigned to.<br><br>After you make your selection, new options may be displayed to define how the door is connected to the panel. |
| **Subpanel** | The subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the selected main panel. |
| **Lock Number** | The number ID for the set of inputs/outputs that are connected from the subpanel to the door.<br><br>This option is only displayed if there are inputs or outputs connected to the selected subpanel. |
| **Door Number** | The number that has been assigned to the door module by the wireless lock configuration device. |
| **APB Mode** | The Anti-Passback (APB) mode for the door.<br><br>For more information on Anti-Passback modes, see *Anti-Passback Modes* on page 205. |
| **APB Delay** | Tthe number of seconds before another APB entry with this badge is allowed. Leave blank for no delay, enter 0 to never allow an entry with this badge until it has been used at another door. |
| **Into Area** | The area that the user enters by passing through the door.<br><br>Only the areas that have been previously configured in the system appear in this list. |
| **Out of area** | The area that the user exits by passing through the door.<br><br>Only the areas that have been previously configured in the system appear in this list. |

| | |
|---|---|
| **PIN Timeout** | The number of seconds that a user is allowed to enter multiple PIN attempts before generating “Deny Count Exceeded” event.<br><br>**Note:** If the PIN Timeout is set to `10` seconds and then the PIN Attempts is set to two, this tells the system, if there are two bad PIN attempts within 10 seconds then generate a Deny Count Exceeded event. |
| **PIN Attempts** | The number of times a user can attempt to enter a PIN within the allotted PIN Timeout time frame before an “Deny Count Exceeded” event is generated. |
| **Strike Mode** | The strike mode.<br><br>• **Cut short when open** — The strike is deactivated when the door opens. This option requires that the door has a door position switch (DPOS) installed to monitor the **Open** and **Closed** door states. This strike mode is used with the **Standard Access Time** setting.<br>• **Turn off on close** — The strike is deactivated when the door closes. This option requires that the door has a DPOS installed to monitor the **Open** and **Closed** door states. This strike mode is used with the **Standard Access Time** setting.<br>• **Full strike time** — The strike is deactivated when the strike timer expires. This strike mode is used with the **Access time when open** setting. |
| **LED Mode** | The LED mode to specify how the reader LEDs are displayed.<br><br>For more information on LED modes, see *LED Modes for Mercury Security* on page 304. |
| **Held Pre-Alarm** | The number of seconds a door can be held open before a pre-alarm is issued. If activated, the 'Door held open pre-alarm' event may be used to send an email notification.<br><br>Example: `20` seconds<br><br>If `120` seconds is entered in Held Open Time, the pre-alarm warning will be sent at 100 seconds and the 'Door held open' event at 120 seconds.<br><br>If `200` seconds is entered in Extended Held Open Time, the pre-alarm warning will be sent at 180 seconds and the 'Door held open' event at 200 seconds.<br><br>For more information, see *Configuring Door Held-Open Settings* on page 192. |
| **Access time when open** | The number of seconds the door remains unlocked after access has been granted.<br><br>**Note:** This setting only applies, and must be configured, when the **Strike Mode** is set to **Full strike time**. |
| **Standard Access Time** | The number of seconds the door remains unlocked after access has been granted.<br><br>If the door is not opened within this time, it will automatically lock.<br><br>**Note:** This time setting only applies, and must be configured, when the **Strike Mode** is set to **Cut short when open** or **Turn off on close**. |

| | |
|---|---|
| **Held Open Time** | The number of seconds a door can be held open before a 'Door held open' event is generated.<br><br>Example: `120` seconds<br><br>For more information, see *Configuring Door Held-Open Settings* on page 192. |
| **Extended Access** | The number of seconds the door remains unlocked after access has been granted to token holders with extended access permissions.<br><br>This feature is useful for users that may require more time to enter a door. |
| **Extended Held Open Time** | The number of seconds a door can be held open for users with extended access permissions before a Door held open' event is generated.<br><br>This feature is useful for users that may require more time to enter a door, such as individuals with accessibility needs.<br><br>Example: `200` seconds<br><br>For more information, see *Configuring Door Held-Open Settings* on page 192. |
| **Card Formats** | Identify the card formats that the door accepts by moving them into the Members column if they are not already listed.<br><br>All of the doors on a panel (and its subpanels) can collectively use at most 16 distinct card formats, from the up to 128 card formats defined for the entire system.<br><br>When the door is created, the initial selection of card formats depends on:<br><br>• If there are 16 or less card formats defined in the system, all card formats are in the Members column.<br>• If there are 17 or more card formats in the system, and:<br>  ◦ No card formats are selected for the panel assigned to the door, then the Members column is empty. You must select the card formats accepted at the door.<br>  ◦ Some door formats are selected for the panel assigned to the door, then those formats are listed in the Members column. You can add more up to a total of 16.<br>• If the door is created using a door template, and the template specifies:<br>  ◦ No Change: The Members column is populated as described above.<br>  ◦ Blank: Any selection from the panel is ignored and the Members column is empty. You must select the card formats accepted at the door.<br>  ◦ Assign: The contents of the Members column from the panel are replaced by the contents of the Members column from the door template.<br>  ◦ Add: Card formats not in the Members column from the panel that are in the Members column of the door template are added, up to a maximum of 16. If there are more than 16, you will have to manually adjust the list.<br>  ◦ Remove: Any card formats in the Members column from the panel that are in Members column of the door template are removed. |
| **Simple Macros** | |
| **Type** | Select a default macro that is triggered when the following conditions are met for this door. Currently available macros include:<br><br>• Forced<br>• Held<br>• Pre-Alarm |

| | |
|---|---|
| **Schedule** | Define when this macro can be triggered.<br><br>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Op Type** | Select an operation type used by this macro. |
| **Output** | Select an output that is activated by the 'Type' condition. |
| **Commands** | Click **Save Macro** to save the settings for this canned macro. If this is a new macro, a new row is automatically added below.<br><br>Click **Remove Macro** to delete a macro. This button only appears if the macro has been saved in the system.<br><br>For more information, see *Adding Simple Macros* on page 200. |

The following options are always active:

| | |
|---|---|
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Create New Report** | Click this button to generate a PDF report on this door. |
| **Add Door** | Click this button to add a new door. |
| **Transaction Report** | Click this button to generate a PDF transaction report on this door. |
| **Show Policy** | Click this button to generate a PDF report on the current door policy. |

### Hardware tab (Mercury Security)

When you click the **Hardware** tab at the Door Edit screen, the Mercury Hardware page is displayed. This page allows you to connect and edit readers, inputs and outputs to the door.

> **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| Feature | Description |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | Specifies the panel the door is assigned to.<br><br>After you make your selection, new options may be displayed to define how the door is connected to the panel. |

| Feature | Description |
|---|---|
| **Subpanel** | Specifies the subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the selected main panel. |
| **Lock Number or Door Number** | The number programmed for the lock. For all locks except SimonsVoss, this is a decimal number. For SimonsVoss wireless locks, this is a hexadecimal number. |
| **Unassign All** | Click this button to reset all of the values below and start over. |
| | To edit one of the readers, inputs or outputs that are connected to the door, click beside the hardware item:<br><br>• If you click beside the Reader or Alternate Reader, the Reader Edit page is displayed.<br>• If you click beside the Door Position, REX #1 or Rex#2, the Input Edit page is displayed.<br>• If you click beside Strike, the Output Edit page is displayed. |
| **Elevators**<br><br>**The following options are only listed if the door is an elevator.** | |
| **Offline Access** | This identifies the floor that this door reader defaults to if communication between the panel/subpanel and the door's reader goes offline. The door will automatically provide access to one or more designated floors or doors, with or without card/code entry, if this condition occurs.<br><br>Select the elevator access level from the drop down list.<br><br>Only the elevator levels that have been defined in the system are listed. |
| **Facility Access** | This identifies the elevator access level that this elevator defaults to if facility code mode is in effect.<br><br>Select the elevator access level you require from the drop down list.<br><br>Only the elevator levels that have been defined in the system are listed. |
| **Custom Access** | This identifies the elevator access level that this elevator defaults to when custom code mode is in effect.<br><br>Select the elevator access level you require from the drop down list.<br><br>Only the elevator levels that have been defined in the system are listed. |
| **Elevator Outputs** | Select the output this elevator uses. |
| **Elevator Inputs** | Select the input this elevator uses. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Create New Report** | Click this button to generate a PDF report on this door. |
| **Add Door** | Click this button to add a new door. |

| Feature | Description |
|---|---|
| **Transaction Report** | Click this button to generate a PDF transaction report on this door. |
| **Show Policy** | Click this button to generate a PDF report on the current door policy. |

# Reader Edit page (Mercury Security)

When you click the icon beside the Reader or Alternate Reader field on the Door Hardware page, the Reader Edit page is displayed. This page allows you to define the options for this reader.

| Feature | Description |
|---|---|
| **Name** | Enter the name of this reader. |
| **Alt.name** | Enter an alternative name for this reader. |
| **Location** | Enter a brief description of the location of this reader. |
| **Reader Type** | Select the communication protocol used by the reader. The options include:<br>• **OSDP**<br>OSDP is recommended for readers, controllers and subpanels communications. OSDP offers support for bi-directional communication, Secure Channel Protocol (SCP) to encrypt the traffic, and provides additional status values for readers, improved LED controls, and simpler wiring.<br>• **F/2F**.<br>• **D1/D0 (Wiegand )**<br>• **CLK+Data (Mag)** ( NCI magnetic stripe standard)<br>• **Custom** (Default)<br>**Note: Custom** enables all options for all reader types. Readers configured with versions of the ACM software earlier than Release 5.10.4 are assigned this reader type when the software is upgraded to ensure that the previous settings are retained. |
| **The following options depend on the selected Reader Type and include:** | |
| **LED drive** | Select the LED drive mode for this reader. The options depend on the reader model and how it is wired and include:<br>• **None**<br>• **Gen 1 wire**<br>• **Reserved**<br>• **Sep Red/Grn no buzz**<br>• **Dorado 780**<br>• **LCD**<br>• **OSDP** |
| **Format by nibble** | Check this box to indicate that this reader supports the format by nibble. |

| Feature | Description |
|---|---|
| **Bidirectional** | Check this box to indicate that this reader can reader bidirectionally. |
| **F/2F Decoding** | Check this box to indicate that this reader uses F or F2 decoding. |
| **Inputs on reader** | Check this box to indicate that this reader provides one or more input ports for serial input arrays. |
| **Keypad decode** | Select the keypad decode/encryption method that is used by this reader. The options include:<br>• **MR20 8-bit tamper**<br>• **Hughes ID 4-bit**<br>• **Indala**<br>• **MR20 8-bit no tamper** |
| **Wiegand** | Check this box to indicate that this reader supports the Wiegand standard. |
| **Trim Zero Bit** | Check this box to indicate that this reader supports the trim zero bit standard. |
| **Secure Channel Protocol** | Check this box to enable secure OSDP communication between the reader and the controller. The reader must support SCP and must be in installation mode. The reader will remain offline if a secure connection cannot be established.<br>**CAUTION —** Do not enable SCP on readers that support OSDPv1, such as the ViRDI biometric reader, as this will make the reader inoperable. Secure channel is only supported in by OSDPv2.<br>**Tip:** If a reader with secured OSDP communication has to be replaced, it must be replaced with a reader that supports OSDPv2. Communication between the replacement reader and the controller must be secured, and the communication between the controller and the other OSDPv2 readers must be resecured. |
| **Baud Rate** | Set the OSDP baud rate. This must be the same for all readers on a single port. Valid values are **9600** (default), **19200**, **38000** or **115200**. If blank is selected, the system will use default settings.<br>**Note:** Mercury controllers may auto-detect the OSDP baud rate. For more information, refer to Mercury documentation.<br>See *Appendix: pivCLASS Configuration* on page 503. |
| **OSDP Address** | Set the OSDP address. This must be different for each reader on a single port. Valid values are **0** (reader 1 default), **1** (reader 2 default), **2**, and **3**. If blank is selected, the system will use default settings.<br>**Note:** Mercury controllers will first try the setting provided and if that does not work, the controller will use default settings. |

| Feature | Description |
|---|---|
| **OSDP Tracing** | Displayed for OSDP readers only. If the box is checked, OSDP address tracing will be logged in the `mercury.txt` appliance log for troubleshooting. |
| **NCI magstripe** | Check this box to indicate that this reader supports the NCI standard for magnetic stripes. |
| **Supervised** | Check this box to indicate that this reader is supervised (outfitted with detection devices) |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

# Input Edit page (Mercury Security)

When you click the icon beside the Door Position or REX # field on the Door Hardware page, the Input Edit page for the subpanel of the door is displayed. This page allows you to define the options for this input.

| Feature | Description |
|---|---|
| **Input** | The name of the input point. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Address** | The read-only address of this point. |
| **EOL resistance** | Select the End of Line resistance of this input.<br><br>Only the EOL resistance that have been defined in the system are listed. |
| **Debounce**[1] | From the drop down list, select the number of units this input should be allowed to debounce. Each unit is approximately 16 ms. |
| **Hold time** | Set the amount of time that the alarm will stay in alarm after returning to normal.<br><br>For example, if the input point goes into alarm, then restores, it will hold it in that alarm state for 1 to 15 seconds after it returns to normal before reporting the normal state. |
| **Cameras** | Select the camera from the window that this input activates if it goes into alarm.<br><br>Only those cameras previously defined for this system appear in this window. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Show Policy** | Click this button to display the policies associated with this input module. |

[1]Due to mechanical properties of a switch, when a switch is closed, there is a period of time in which the electrical connection "bounces" between open and closed. To a microcontroller, this "bouncing" can be interpreted as multiple button pushes. To suppress the "bouncing", the controller software is designed to anticipate it. This is known as "debouncing a switch".

# Output Edit page (Mercury Security)

When you click the icon beside the Strike field on the Door Hardware page, the Output Edit page for the subpanel of the door is displayed. This page allows you to define the options for this output.

| Feature | Description |
|---|---|
| **Output** | Enter a name for this output. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Address** | The read-only address for this output point. |
| **Operating Mode** | Select how the panel knows when the output point is active.<br>• **Energized When Active** – a current is expected to pass through the output point when it is *active*.<br>• **Not Energized When Active** – a current expected to pass through the output point when it is *inactive*. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Show Policy** | Click this button to display the policies associated with this output point. |

### Elev tab (Mercury Security)

When you click the **Elev** tab at the Door Edit screen, the Mercury Security Elev table displayed. This page allows you to view elevator door details.

| Feature | Description |
|---|---|
| **Name** | Name of the elevator door. If you click on the name it links back to the Parameters tab for the door. |
| **Inputs** | List of inputs for the related elevator input module. |
| **Outputs** | List of outputs for the related elevator output module. |

### Cameras tab (Mercury Security)

When you click the **Cameras** tab on the Door: Edit screen, the Camera page is displayed. From this page, you can assign specific cameras to record video of the selected door.

**Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| Feature | Description |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |

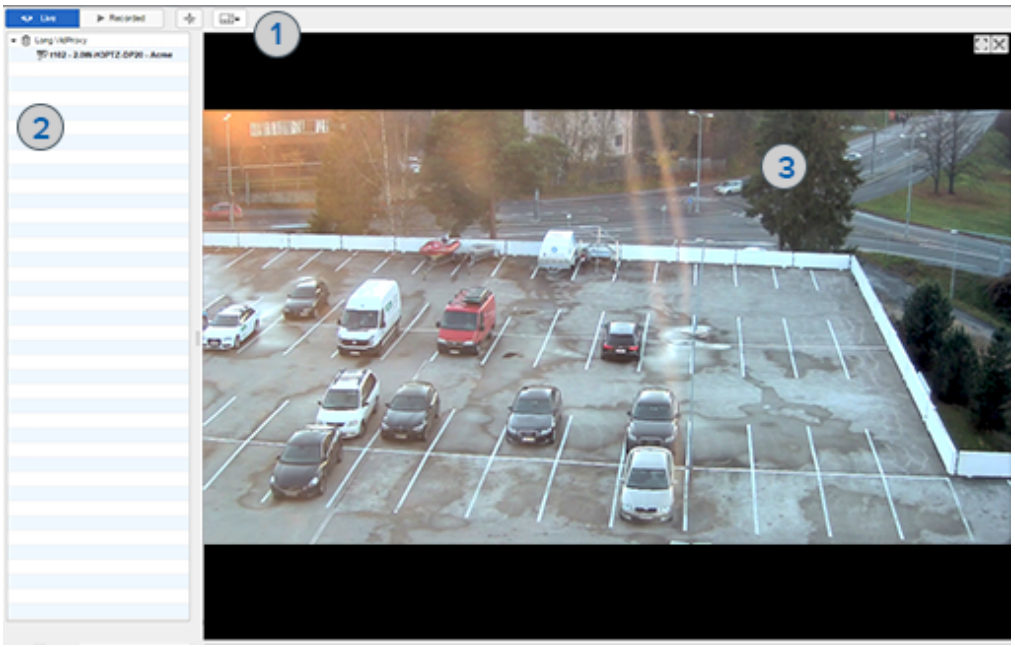
| Feature | Description |
|---|---|
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Panel** | Specifies the panel the door is assigned to.<br><br>After you make your selection, new options may be displayed to define how the door is connected to the panel.<br><br>Not applicable to Avigilon doors. |
| **Subpanel** | Specifies the subpanel that is connected to the door.<br><br>This option is only displayed if there is a subpanel connected to the selected main panel.<br><br>Not applicable to Avigilon doors. |
| **Lock Number** | Enter the number ID for the set of inputs/outputs that are connected from the subpanel to the door.<br><br>This option is only displayed if there are inputs or outputs connected to the selected subpanel. |
| **Door Number** | The number that has been assigned to the door module by the wireless lock configuration device. |
| **Camera Type** | Select the external system that is connected to the camera.<br><br>The Available window is populated with those cameras that fit this definition.<br><br>Click the **Camera** button beside this field to view live video from the camera. For more information on the video viewer window, see *Configuring and Viewing Live Video Stream* on the next page. |
| **Available** | This window displays a list of cameras that have been configured in the system.<br><br>To connect a camera to the door, select the camera from the Available list, then click ► to move it to the Members list. |
| **Members** | The window displays a list of cameras that are currently connected to the door.<br><br>To disconnect a camera from the door, select the camera from the Members list, then click ◄ to move it to the Available list. |
| **Search** | If you have more than 10 cameras, the Search feature may be displayed to help you find the cameras you need.<br><br>In the **Search** field, enter the name of the camera you want to find, then click **Filter**. You can narrow your search by selecting the **Case-sensitive** option. Click **Clear** to restore the full list of available cameras. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |
| | Click this button to generate a PDF report on this door. |

| Feature | Description |
|---|---|
| **Add Door** | Click this button to add a new door. |
| **Transaction Report** | Click this button to generate a PDF transaction report on this door. |
| **Show Policy** | Click this link to view a PDF report indicating the current policy associated with this door. |

# Configuring and Viewing Live Video Stream

## Overview

You can view the LIve Video window in ACM, if configured.




Typically, the Live Video window includes:

| | | |
|---|---|---|
| 1 | **Camera Controls Tool Bar** | Displays controls for viewing the related camera video, including switching from live to recorded video, pan-tilt-zoom (PTZ) controls for PTZ cameras and changing the video display layout. |
| 2 | **Camera List** | Displays all the cameras that are linked to the event. Click the name of a camera to display the video. Use one of the multi-video layouts to display more than one camera at a time. |
| 3 | **Image Panel** | Displays the video stream from the connected cameras. In the top-right corner, you can minimize and maximize the display or close the video. |

**Note:** The window may look different and have different controls depending on the external camera system that is connected to the ACM system.

## Configuring Live Video Stream

To configure live video stream from connected cameras:

1. Selects **Physical Access** > **Doors**.
2. Select the name of the door.
3. On the **Cameras** tab, select:

| | |
|---|---|
| **Camera Type** | The external system that is connected to the camera: **Network**, **Exacq**, **Avigilon** or **Milestone**. Move the cameras to the **Members** column. |

4. Click to save your changes.

   Click to discard your changes.
5. Click the **Camera** button to view live video from the camera.

**Interlocks tab (Mercury Security Doors)**

When you click the **Interlocks** tab on the Door: Edit screen, the Interlocks list is displayed. This page lists all the Interlocks that have been added to the system.

| Feature | Description |
|---|---|
| **Name** | The name of the interlock.<br><br>Click the name to edit the interlock. |
| **Enabled** | This field indicates if the interlock is enabled. Select either Yes or No. |
| **Schedule** | This field indicates what schedule is used to define when the interlock is active. |
| **Delete** | Click to delete this interlock from the list. |
| **Add Interlock** | Click this button to add a new interlock to the system. |

# Interlocks Add page

When you click **Add Interlock** from the Interlocks list, the Interlocks Add page is displayed. Depending on what settings you choose, some of the listed options may not be displayed.

| Feature | Description |
|---|---|
| **Name** | Identifies the interlock.<br><br>Enter a unique name for the interlock. |
| **Enabled** | Check this box to specify that the interlock is enabled and active. |
| **Schedule** | Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Source Type** | Identifies the source type of the interlock.<br><br>Select the source type from the drop down list. |
| **Source** | Identifies the source of the interlock.<br><br>Select the source from the drop down list. Options in this drop down list will vary depending on the source type specified. |

| Feature | Description |
|---|---|
| **Event Type** | Identifies the event type the interlock is associated with.<br><br>Select the Event Type from the drop down list. The options change to match the selected source option.<br><br>Only those Event Types currently defined by the system appear in this list. |
| **Event** | Select the event that will trigger the interlock.<br><br>Events appearing in this list vary depending on the event and source specified. For more on this, refer to Event Types - Introduction. |
| **Interlocks with:** | |
| **Type** | Select the type of component that triggers this interlock. |
| **Subpanel** | If applicable, select from the drop down list the subpanel where this interlock is triggered. |
| **Target** | From the drop down list, select the target that is triggered by this interlock. |
| **Command to run:** | |
| **Command** | This identifies the command script to be run.<br><br>Select an existing command from the drop down list.<br><br>Only those commands previously defined by the system appear in this list. |
| **Function** | If applicable, select from the drop down list the function to be run. |
| **Arg Text** | If the command requires an argument, enter the required argument in this text box.<br><br>This option is not displayed if an argument is not required. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

# Interlock Edit page

When you click the name of an interlock from the Interlocks  list, the Interlock Edit page for the door is displayed.

| Feature | Description |
|---|---|
| **Name** | Identifies the interlock.<br><br>Enter a unique name for the interlock. |
| **Enabled** | Check this box to specify that the interlock is enabled and active. |
| **Schedule** | Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. |
| **Source Type** | Identifies the source type of the interlock.<br><br>Select the source type from the drop down list. |
| **Source** | Identifies the source of the interlock.<br><br>Select the source from the drop down list. Options in this drop down list will vary depending on the source type specified. |

| Feature | Description |
|---|---|
| **Event Type** | Identifies the event type the interlock is associated with.<br><br>Select the Event Type from the drop down list. The options change to match the selected source option.<br><br>Only those Event Types currently defined by the system appear in this list. |
| **Event** | Select the event that will trigger the interlock.<br><br>Events appearing in this list vary depending on the event and source specified. For more on this, refer to Event Types - Introduction. |
| **Interlocks with:** | |
| **Type** | Select the type of component that triggers this interlock. |
| **Subpanel** | If applicable, select from the drop down list the subpanel where this interlock is triggered. |
| **Target** | From the drop down list, select the target that is triggered by this interlock. |
| **Command to run:** | |
| **Command** | This identifies the command script to be run.<br><br>Select an existing command from the drop down list.<br><br>Only those commands previously defined by the system appear in this list. |
| **Function** | If applicable, select from the drop down list the function to be run. |
| **Arg Text** | If the command requires an argument, enter the required argument in this text box.<br><br>This option is not displayed if an argument is not required. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

### Events tab

For Mercury Security, VertX and Avigilon doors

View door events on the **Events** tab in **Physical Access**.

This page lists all the local and global events that can be triggered by this door. The Local Events table is only listed when there are local events configured for the door.

**Local Events**

This table is only displayed if there are local events for the device.

| | |
|---|---|
| **Name** | The name of this event.<br><br>Click the name to edit the local event. |
| **Event** | The event type. |
| **Source Type** | The source of this event. |
| **Has On/Off** | If the event toggles on or off.<br><br>Click **Yes** or **No**. |
| **Masked** | If the event is masked.<br><br>Click to change status to (yes) or (no). |

| | |
|---|---|
| **Logged** | If the event is logged.<br><br>Click to change status to (yes) or (no). |
| **Show Video** | If a video is available for the event. If 'yes' is selected, the live video window automatically pops up when the event is received.<br><br>Click to change status to (yes) or (no). |
| | Click this button to delete the local event. |

**Global Events**

This table displays all the global events that are related to this type of device.

| | |
|---|---|
| **Name** | The name of this event. |
| **Event** | The event type. |
| **Source Type** | the source of this event. |
| **Has On/Off** | If the event toggles on or off.<br><br>Click **Yes** or **No**. |
| **Masked** | If the event is masked.<br><br>Click to change status to (yes) or (no). |
| **Logged** | If the event is logged.<br><br>Click to change status to (yes) or (no). |
| **Show Video** | If a video is available for the event. If 'yes' is selected, the live video window automatically pops up when the event is received.<br><br>Click to change status to (yes) or (no). |
| **Create Local** | Click this button to create a version of this global event that only applies to the specific device. |

# Doors - Creating Local Events for Mercury Security Doors

When you click the **Create Local** button from the Door Events page, the local version of the Event page is displayed. This page is a copy of the global event that can be customized as a local event for this specific door.

> **Note:** Changes on this page do not affect the global event.

Make any changes as required.

| Feature | Description |
|---|---|
| **Name** | The name of the event, which you can change if the name is not. |
| **Return Name** | The name used to identify that this event is over, or the return-to-normal (RTN) ) name of this event, such as the door closing and locking after access has been granted, or after the configured door open time has expired. |

| Feature | Description |
|---|---|
| **Event Type** | The event type.<br><br>Only events types that have been defined in the system appear in the drop down list. |
| **Source Type** | The device that is the source of the event. |
| **Priority** | The priority of this event.<br><br>The priority range is 1 - 999.<br><br>The Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. |
| **Alarm Sound** | A sound that is played when a new alarm occurs while you are monitoring the Alarms page.<br><br>**Note:** A default beeping sound is played, if no sound is selected. |
| **Suppress Time** | A schedule when alarm events are not reported.<br><br>Only schedules that have been defined in the system are listed. |
| **Instructions** | Any instructions that may be required for handling this event.<br><br>The instructions are made available to the user on the Monitor screen. |
| **Return Event** | The event type of the RTN event. |
| **Return Priority** | The priority of the RTN event.<br><br>The priority range is 1 - 999. |
| **Has on/off** | This event has an RTN event associated with it.<br><br>**Note:** Adding return event information manually on this screen does not change the setting of this checkbox. It is set only if the original event has an associated RTN event defined for it. |
| **Masked** | This box indicates that this a masked event by default. This can be changed on the Event List page. |
| **Logged** | This box indicates to log the event by default. This can be changed on the Event List page.<br><br>Note that if Event Type logging is turned on, then all Events of that Event Type are logged, regardless of their individual logging configuration. If Event Type logging is turned off, then the logging configuration of the specific Events of that Event type are adhered to. |
| **Show Video** | This box indicates to auto-launch video from the linked camera feed when the event occurs by default. This can be changed on the Event List page.<br><br>This feature only works if video is enabled. |
| **Two Person Required To Clear** | This box indicates that two people are required to acknowledge and clear this event.<br><br>If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge.<br><br>If the same operator attempts to clear the alarm, then nothing will happen. |

| Feature | Description |
|---|---|
| **Email** | The email address of all the people who should be notified when this event occurs.<br><br>You can enter more than one email address separated by a comma. |
| **Roles:** | |
| **Available** | A list of all the roles that are available to you in the system.<br><br>To allow specific role to have access to view or edit this event, select a role from the Available list then click ▶ to add the role to the Member list.<br><br>To move one or more roles to the Members window, click to select one role then **Ctrl** + click to select a non-consecutive group of roles, or **Shift** + click to select a consecutive roles. |
| **Members** | A list of all the roles that are able to view or edit this event.<br><br>If this event is associated with at least one role, then any user who does not have the selected roles will not be able to view or edit the event. |

### Access tab (Mercury Security)

When you click the **Access** tab on the Edit screen, the Access page is displayed. This page provides a list of the access groups, roles and identities that have permission to edit or use this door.

| Feature | Description |
|---|---|
| **Access Group** | The name of this access group. Click this link to edit the access group. |
| **Roles** | Lists the roles this access group is a member of.<br><br>Click the **+** or **-** symbol beside each role to show or hide the identities that are in the access group through the role. |
| **Identities** | Lists the users who are members of the access group. |

### Transactions tab (Mercury Security)

When you click the **Transactions** tab on the Door: Edit screen, the list of transactions for the door is displayed.

This page allows you to review events and alarms that have occurred at this door. The table displays the following information about each event:

| Feature | Description |
|---|---|
| **Panel Date** | The date and time when the event occurred. |
| **Priority** | The priority of the event. The highest priority is 1 and the lowest priority is 999. |
| **Event** | The name of the event. |
| **Last Name** | The last name of the person who generated the event. |
| **First Name** | The first name of the person who generated the event. |
| **Card Number** | The internal token number assigned to the person who generated the event. |
| **Message** | This displays any messages that may be associated with the event. |

## Doors - Access page

The door access page is found on every version of the door. The access page for each manufacturer is:

- Doors - Mercury Security Door Access
- Doors - HID VertX® Access

## Viewing Door Events, Access Groups and Transactions

To view access information, events and alarms generated for doors:

1. Select **Physical Access** > **Doors**.

   For more information about door state and door mode, see *Adding Doors* on page 214.

   For event descriptions, see *Troubleshooting* on page 490.
2. Select the name of the door.
3. Click the **Events** tab to view all the global events that are related to the device:

| | |
|---|---|
| **Name** | The name of the event. |
| **Event** | The type of event. |
| **Source Type** | The source of this event. |
| **Has On/Off** | If the event toggles on or off.<br>Click **Yes** or **No**. |
| **Masked** | If the event is masked.<br>Click to change status to (yes) or (no). |
| **Logged** | If the event is logged.<br>Click to change status to (yes) or (no). |
| **Show Video** | If a video is available for the event. If 'yes' is selected, the live video window automatically pops up when the event is received.<br>Click to change status to (yes) or (no). |

> **Tip:** You can also view events using **Monitor** > **Events**. For more information, see *Monitoring Events* on page 26.

4. Click the **Access** tab to view the access groups, roles and identities that have permission to edit or use the door (not applicable to RU and RM exit devices):

| | |
|---|---|
| **Access Groups** | The name of the access group. Click the link to edit the access group. |
| **Roles** | The roles that the access group is a member of. Click the + or - icon next to each role to show or hide the identities in the access group through the role. |
| **Identities** | The users who are members of the access group. |
| **Panel Date** | The date and time when the event occurred. |
| **Priority** | The priority of the event. The highest priority is 1 and the lowest priority is 999. |
| **Event** | The name of the event. |
| **Last Name** | The last name of the person who generated the event. |
| **First Name** | The first name of the person who generated the event. |
| **Card Number** | The internal token number assigned to the person who generated the event. |

| | |
|---|---|
| **Message** | Any messages that are associated with the event. |

For more information, see *Managing Door Access* on page 105.

5. Click the **Transactions** tab to view the events and alarms that have occurred at the door:

| | |
|---|---|
| **Access Groups** | The name of the access group. Click the link to edit the access group. |
| **Roles** | The roles that the access group is a member of. Click the + or - icon next to each role to show or hide the identities in the access group through the role. |
| **Identities** | The users who are members of the access group. |
| **Panel Date** | The date and time when the event occurred. |
| **Priority** | The priority of the event. The highest priority is 1 and the lowest priority is 999. |
| **Event** | The name of the event. |
| **Last Name** | The last name of the person who generated the event. |
| **First Name** | The first name of the person who generated the event. |
| **Card Number** | The internal token number assigned to the person who generated the event. |
| **Message** | Any messages that are associated with the event. |

For more information, see *Configuring Roles* on page 82.

# Configuring ACM Verify™ Virtual Doors

The ACM Verify function allows authorized ACM system users to connect any web browser-enabled mobile device to the ACM system and use the device as a virtual station for a door configured as an ACM Verify Station. A virtual station controls access to places that do not have access-controlled doors or locks. Examples are outdoor mustering stations for fire drills, a bus for school trips or a work area in an open-plan office. People entering a place controlled by a virtual station must verify they are authorized to access the area by entering their PIN code on the device. Typically, wireless web browser-enabled devices, such as mobile phones and tablets, are used as virtual stations although any device with a web-browser can be used.

ACM system users assigned the ACM Verify Administrator role can add and configure doors as ACM Verify stations, and administer the virtual stations and paired devices in the ACM system. They can also administer other doors.

ACM system users assigned the ACM Verify User role can access the ACM Verify functionality on their mobile devices that let the devices act as virtual stations, and can pair their mobile device to the ACM system.

## Adding an ACM Verify Door

To set up a door as an ACM Verify Station

1. Add a new door from the Doors listing panel, and complete the Name, Alt Name, Location and Appliance fields.
2. In the Vendor field, select Avigilon. The Station Type field is automatically set as ACM Verify.
3. Configure the station as either Managed or UnManaged,
    - A managed station prompts the operator of the virtual station to verify that the person who enters a PIN code is using a valid PIN code and it also displays a picture and other information for additional verification.
    - An unmanaged station only verifies whether the PIN code the person entered is a valid PIN code that has access to the virtual station.

4. Set the timezone for the events reported by the virtual station if it needs to be different than the timezone used by the appliance.
5. Specify an area if you want the virtual station to act as an entrance to the area.

   If the virtual station is configured with an area, a valid PIN code entry at the station moves the identity associated with the PIN code into the area. If it also configured as a managed virtual station, the user can then view a list of the identities with photos that are in the area.
6. Configure Station Authorization as Paired or Login
   - A paired station is secured by pairing a specific device to the server so that only an ACM software user in possession of the paired device and one of the required roles, or their equivalent delegation set can access the ACM Verify station.
   - A login station is secured only by ACM login credentials and so that any ACM system user with the required roles, or their equivalent delegation set, can access the ACM Verify station from any device.
7. If Station Authorization is set to Paired, two lists are displayed. The Available list displays devices paired to the ACM appliance but not assigned to this door. The Members list displays the paired devices assigned to this door. Use the ◄ and ► keys to move devices between the two lists.
8. To pair a new device to the ACM appliance, click Add Paired Device. For more information, see *Paired Devices* on the next page.
9. Click ✔ to save the door. The page refreshes and displays the information you entered on Parameters tab for the door.

## Parameters tab (Avigilon)

After you save a new door as an ACM Verify Station for the first time, the screen refreshes and displays the initial Parameters tab for the door.

When you click the **Parameters** tab on the Door Edit screen, the Parameters page is displayed. This page allows you to define the door connections, door mode, schedule and processing attributes.

| Feature | Description |
|---|---|
| **Name** | The name of the door. |
| **Alt Name** | The alternative name of the door. |
| **Location** | The location of the door. |
| **Appliance** | The appliance the door is connected to. |
| **Vendor** | The name of the door manufacturer. Select Avigilon for an ACM Verify Station. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Station Type** | Displays ACM Verify as the type of station used on the connected devices. A device that uses this type of station is called a virtual station. |
| **Managed or UnManaged** | Select if you want the ACM Verify Station managed or not.<br>• A managed station requires the virtual station user to grant or deny access to the person entering a valid PIN code. It also displays the name and picture of the user for verification.<br>• An unmanaged station automatically grants or denies access and does not provide any additional information when a PIN code is entered. |
| **Geographic Timezone** | Select the time zone where the ACM Verify device is used if it is different from the ACM appliance value. |

| Feature | Description |
|---|---|
| **Into Area** | Select the area where the ACM Verify device is used to monitor access. Select the Don't Care option if the ACM Verify reader is not used to control access to a specific area. You must specify an area if you want the virtual station to list all the people who have entered the area. |
| **Station Authentication** | Select Login if the user logs in to the ACM software using the ACM URL from the browser on the ACM Verify device. Select Paired if the ACM Verify device is paired to ACM software.<br><br>**Tip:** If the authentication type is Paired, the Door Add page re-displays with the Add Paired Device button. |
| **Available** | Lists the available ACM Verify devices that have been paired to the ACM system. |
| **Members** | Lists the paired ACM Verify devices that are assigned to this station. |
| ▶ | Click to move a paired device from the Available list to the Members list. |
| ◀ | Click to move a paired device from the Members list to the Available list. |
| **Add Paired Device** | Click to add a new paired device. See Add Paired Device for more information. |
| ✔ | Click this button to save your changes. |
| ✖ | Click this button to discard your changes. |

# Paired Devices

Pairing devices to the ACM appliance ensures that access to ACM Verify Stations is restricted to authorized devices.

Pairing must be completed by both the ACM administrator and the user of the connected device. The device user must be an authorized ACM user with the ACM Verify User role or equivalent at a minimum. The pairing persists as long as the cookie used for the pairing exists. See *Precautions for Paired ACM Verify Stations* on the next page

**CAUTION —** In a failover deployment of the ACM system, pair the device to both the main server and the failover server. When a failover occurs, the ACM operator must restore the pairings for all ACM Verify devices to the failover server, and repeat the process when the main server is back in service.

## Prerequisites for Pairing Devices

Before pairing a device:

1. The ACM operator provides the user with the IP address or hostname of the ACM appliance. Do not provide both. Use one format for the address of the ACM appliance for all pairings.

   The ACM appliance IP address or hostname is visible in the web browser's navigation bar from any ACM client window.
2. The device user must have the web browser open on their device.

The pairing must be completed within ten minutes of the ACM operator generating the PIN for pairing.

Although the user's device is paired to the ACM appliance, the virtual stations configured for paired authentication are only active for a device when installed and the user's device is in the Members column for

that station.

A device can be paired to only one active ACM appliance. If a failover ACM appliance is configured, pair all ACM Verify devices to both servers. If a fail-over occurs, you must reassign devices to the ACM Verify stations on the fail-over server while it is active, and reassign them back to the main server after it is returned to service. Pairing devices in advance will make this task much more efficient.

To pair a device, see *Pairing a Device* below.

## Precautions for Paired ACM Verify Stations

A paired device uses cookies to connect to ACM. Take the following precautions:

- Always use the same device and browser to connect. Cookies are not shared between different devices or browsers.
- Do not pair the device while in private mode on your browser. Cookies are not saved when you are in private mode.
- Cookies are lost if you:
  - Clean up history and cookies in your browser
  - Pair the device using an IP address and then use the host name to access ACM.

If a device browser loses the cookie, it cannot access ACM Verify and you must pair the device again. Before the device can be paired again, the previous pairing must be deleted from the ACM appliance.

## Pairing a Device

A device needs to be paired to the ACM appliance to access the ACM Verify function. A device can be paired to the ACM appliance at any time, or when adding a door as an ACM Verify Station.

To pair a device:

1. The ACM operator and the device user agree on the name to use for the device.
2. The ACM operator provides the ACM URL or hostname to the device user.

   The ACM appliance IP address or hostname is visible in the web browser's navigation bar from any ACM client window.
3. The ACM operator navigates to the Add Paired Device panel.
   a. If the operator is:
      - Pairing a device only, click > **Paired Devices**.
      - Adding a new door as an ACM Verify Station, click on **Add Paired Device** in the Door: Add New screen. For more information, see *Parameters tab (Avigilon)* on page 262.
   b. Enter the name to identify the device, such as "User Name's Smartphone" and click **Generate PIN**.

   Provide the 4-digit PIN to the device user. The PIN is valid for 10 minutes.
4. The device user:
   a. Enters the URL to the ACM appliance in the web browser on their device in the format:
      `<ipAddress>/doors/virtual`
      The ACM client log in screen is displayed.
      For example, if the ACM URL is 192.168.0.125, the device user enters:
      `//192.168.0.125/doors/virtual`
   b. Logs in to the ACM Verify client using their username and password.

c. Clicks on the and then clicks >**Paired device**.
The user is prompted to enter the name of their device and the 4-digit PIN provided by the ACM operator.

5. The ACM operator waits until the device is paired and then clicks .

To remove a pairing from the ACM appliance, click for the device.

## Using ACM Verify

You can use a web browser-enabled device, such as a smartphone or tablet, to connect to ACM, access the ACM Verify Station functionality and use the device as a virtual station. Virtual stations control access to places that do not have access-controlled doors or locks. Examples are outdoor mustering stations for fire drills, a bus for school trips or a work area in an open-plan office. People entering a place controlled by a virtual station must verify they are authorized to access the area by entering their PIN code on the device.

You must be an ACM user to use ACM Verify on your device. To set up a device for ACM Verify, see *Configuring ACM Verify™ Virtual Doors* on page 261.

To use ACM Verify:

1. Use the URL or web link in your web browser provided when your device was set up to launch ACM Verify from your web browser.

   **Note:** If your device is paired to the ACM user, always use the same browser.

2. If the Access Control Manager login page is displayed, enter your ACM Login and Password.

   ACM Verify is displayed and the Virtual Stations you can use are listed.

3. Tap to open a virtual station.

   A prompt to enter PIN codes appears.

4. Anyone wanting to access the location you are controlling must enter a PIN code on your device and tap **Submit**.
   - If the virtual station is managed, the user's picture and name displays, and you are prompted to grant or deny access.
   - If the virtual station is unmanaged, access is granted if the code is valid.
   - If the PIN code is incorrect or invalid, a message that access is not granted displays.
5. If an area is specified for the virtual station, the number of identities verified is also displayed, and you can display a list of all the identities who have entered the area by clicking on the **Identities Verified:** link.
6. To switch to a different virtual station, tap the back button and tap another virtual station.

   For example, if you want to have identities enter and exit an area using their PIN codes you need two virtual stations. One station is configured for the area you want identities to enter into, and the second station is configured for the area you want identities to exit into. Both virtual stations are accessible on the same device.

To log out of ACM Verify, tap and tap **Log Out**.

# IP/PoE Mode Installation

Add a Schlage ENGAGE™ site in ACM to configure and manage groups of Schlage® IP-enabled devices through the Schlage ENGAGE™ Gateway that supports IP/PoE (Power over Ethernet) mode of operation. For more information, see:

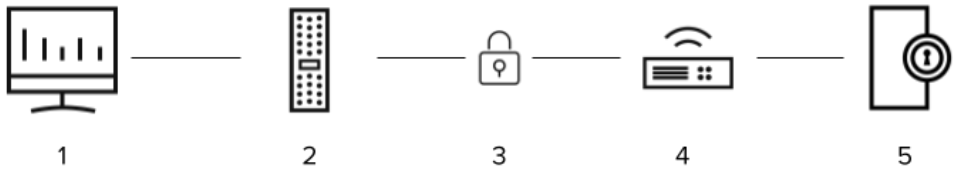
- *System Overview* below
- *Supported Devices* below
- *Step 1: Creating an ENGAGE Site* on page 276
- *Step 2: Configuring Gateways for IP-enabled Wireless Locks* on page 268
- *Step 3: Configuring IP-enabled Wireless Devices* on page 269
- *Step 4: Configuring Locking Operation* on page 270

**Note:** ACM supports only the Schalge and Von Duprin® devices in *Supported Devices* below in IP/PoE mode. Other device models might not operate correctly.

**Tip:** If you are installing Schlage Wi-Fi locks, see *Offline Wi-Fi Mode Installation* on page 275.

## System Overview

**Figure 4:** ACM System organization for Allegion Schlage® IP/PoE wireless locks




| | |
|---|---|
| 1 | ACM applications, including identity (badging), administration, video surveillance and alarm monitoring |
| 2 | ACM appliance |
| 3 | Encrypted connection provided by the Schalge ENGAGE site that the ENGAGE gateway is commissioned to (the site is created in ACM) |
| 4 | ENGAGE gateway panel that supports up to 10 IP-connected devices in any combination using IP (410-IP)/PoE (Power over Ethernet) mode of operation, or ASSA ABLOY Aperio IP hub panel that supports up to 64 IP-connected devices. |
| 5 | Schlage IP wireless locks including mobile-enabled and Allegion Von Duprin remote undogging (RU) and remote monitoring (RM) exit devices |

## Supported Devices

Ensure the physical configuration of the device matches the configuration in the ACM application as follows.

**Note:** Up to 10 IP-connected devices—in any combination—are supported by a single gateway.

| Door<br><br>Linked Device | Panel | Subpanel | External System |
|---|---|---|---|
| *Allegion Schlage LE and NDE series* | | | |
| Up to 10 wireless locks to each gateway<br><br>Up to 5000 credentials to each lock<br><br>Up to 10 mobile-enabled wireless locks to each gateway<br><br>Mobile credentials are not supported. | Up to 1,024 panels to an ACM appliance<br><br>An ENGAGE gateway is a panel. | - | ENGAGE site |
| *Allegion Schlage Control™ smart locks* | | | |
| Up to 10 wireless locks to each gateway<br><br>Up to 500 credentials to each device | Up to 1,024 panels to an ACM appliance<br><br>An ENGAGE gateway is a panel. | - | ENGAGE site |
| *Allegion Von Duprin remote undogging (RU) and remote monitoring (RM) devices* | | | |
| Up to 10 RU or RM devices to each gateway<br><br>Single door configuration only.<br><br>Credentials are not applicable. | Up to 1,024 panels to an ACM appliance<br><br>An ENGAGE gateway is a panel. | - | ENGAGE site |

## Step 1: Creating an ENGAGE Site

**Note:** Before you begin, obtain the ENGAGE login account information. For more information, see Schlage documentation.

To create an ENGAGE site in ACM:

1. Select >**External Systems**.
2. Click the **Schlage** tab.
3. Click the **Add Schalge Site** button.
4. Enter:

| | |
|---|---|
| **Site Name** | Up to 50 alphanumeric characters for the name of the site which represents the logical group of ENGAGE devices.<br><br>**Note:** Always create an ENGAGE site in the ACM application. A site that is already created in the ENGAGE application cannot be reused in the ACM application. In addition, a site cannot be used by more than one ACM appliance. |
| **ENGAGE User** | The login name of the ENGAGE account. |
| **ENGAGE Password** | The password of the ENGAGE account. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |

5. Click to save your changes.

   Click to discard your changes.

After you add the ENGAGE site for an IP-connected lock, see *Step 2: Configuring Gateways for IP-enabled Wireless Locks* below.

After you add the ENGAGE site for an offline Wi-Fi lock, see *Step 2: Setting Up Communication to Offline Wi-Fi Locks* on page 277.

## Step 2: Configuring Gateways for IP-enabled Wireless Locks

For Schlage gateways that control Schlage IP-enabled wireless devices.

To configure a Schlage gateway:

1. Ensure gateway communication to the ACM appliance is enabled:
   a. Select > **Appliance** and the **Access** tab.
   b. Select the **Installed** checkbox next to the **Schalge** vendor.
   c. Click .
   d. Contact your support representative to enable the Debug checkbox, if needed.
2. Select **Physical Access>Panels**.
3. Click **Add Panel**.
4. Enter:

| | |
|---|---|
| **Name** | Up to 50 characters for the name of the gateway. |
| **Physical Location** | A description of where the device is installed. |

| | |
|---|---|
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Appliance** | The ACM appliance the device is connected to. |
| **Vendor** | Select **Schlage**.<br>**Model**: **ENGAGE Gateway - IP**.<br>**Site** : The name of the site that the gateway is commissioned to.<br>**Timeszone** : The local timezone where the gateway is installed. |

5. Click ✔ to save your changes. The entries are displayed on the **Configure** tab.
6. Click the **Host** tab.
7. Enter:

| | |
|---|---|
| **IP Address** | The IP address of the gateway or hostname of the device. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |

8. Click ✔ to save your changes.

After gateway communication is enabled, any devices linked to the gateway will be displayed in the following places:

- On the **Status** tab of the abovementioned panel page, where the **Link Name**, **S/N** (serial number), **Status** (of the connection to each device) and **Credential Capacity** (for each device that supports credentials) columns are displayed.
- In the **Linked Devices** field on the door page.

For more information, see *Step 3: Configuring IP-enabled Wireless Devices* below.

## Step 3: Configuring IP-enabled Wireless Devices

For Schlage IP-enabled wireless devices.

> **Note:** Before you begin, ensure the devices have been installed according to the vendor's installation instructions. If you are not ready to physically install the devices, you can predefine doors as described in this section without specifying the devices.

To configure a wireless device:

1. Ensure device communication is supported in ACM software:
   - Add the ENGAGE site in ACM, as described in *Step 1: Creating an ENGAGE Site* on page 276.
   - Add a gateway for Schlage IP wireless devices, as described in *Step 2: Configuring Gateways for IP-enabled Wireless Locks* on the previous page.
2. On the Panel: Status or Doors list page, do one of the following:
   - Click **Add Door** to create a new door for each new device. Click **Cancel** in the Templates dialog.
   - Select the name of a device linked to the gateway.

3. On the **Parameters** tab, select:

| | |
|---|---|
| **Vendor** | **Schalge**. |
| **Panel** | The gateway. |
| **Lock Model** | The lock model. See *Supported Devices* on page 266. |
| **Linked Device** | The ID or name of each externally commissioned IP wireless or offline Wi-Fi device. For more information, refer to the commissioning process in vendor documentation.<br>**Tip:** IP wireless device only. You can save the door without a linked device and enter it as a post-installation step. |
| **Access Type** | IP-connected wireless device only. Whether access is located on one or both sides of the door. Default is **Single**, which cannot be changed. For more information, see *Access Types* on page 204. |
| **Door Mode** | IP-connected wireless device only. The entry mode for the door when the gateway is online and communicating with the device. For information about the **Unlocked**, **Locked No Access** and **Card Only** options, see *Door Modes* on page 203.<br>Door modes are device-specific and not applicable to Control locks. |
| **Lock Function** | None is the default. For more information about the **Privacy**, **Apartment** and **Office** lock functions, see *Adding Doors* on page 214.<br>Lock function is device-specific. |
| **Always Mask Forced** | The Door Forced Open alarms at the door are always masked. |
| **Always Mask Held** | The Door Held Open alarms at the door are always masked. |
| **Door Processing Attributes** | For more information about the **Log Grants Right Away**, **Log All Access as Used** and **Detailed Events** door processing attributes, see *Adding Doors* on page 214.<br>Not applicable to Control locks. |

4. Click ✔ to save your changes.

After you add a new door, customize other door settings to meet your system requirements. For more information, see *Step 4: Configuring Locking Operation* below.

## Step 4: Configuring Locking Operation

For Schlage IP wireless locks that do not support in/out readers, and RU or RM devices.

To configure locking operation:

1. Edit device settings as required:

   (The **Name** through **Installed** fields can be edited on the Parameters, Operations and Cameras tabs. For these field descriptions, see *Adding Doors* on page 214.)

   On the **Operations** tab, select:

| | |
|---|---|
| **Into Area** | The area that the badge holder enters by passing through the door.<br>Example: Laboratory<br>For more information, see *Adding Areas* on page 301. |
| **Out of area** | The area that the badge holder leaves by passing through the door.<br>Example: Lobby<br>For more information, see *Adding Areas* on page 301. |
| **Standard Access Time** | The seconds the door remains unlocked after access has been granted. |
| **Held Open Time** | The seconds the door can be held open before a Door Held Open event is generated. |
| **Extended Access** | The seconds the door remains unlocked after access has been granted to token holders with extended access permissions. |
| **Card Formats** | **Important:** To maximize the security and capacity of your locks, only move the card formats that are actually used to the **Members** column.<br>Make sure the **Facility Code** in Physical Access > Card Formats matches the facility code on the card. This ensures credential matching occurs during card operation on the door that uses the card format. For more information, see *Configuring Card Formats* on page 305.<br>**Note:** The **Suppress facility check** checkbox must not be used. |

2. Click ✔ to save your changes.
   Allow time for the device configuration to take effect.

   **Important:** Check the credential capacity of the door on the Panel: Status tab before you add more credentials to the lock.

3. Does not apply to Control locks. Add the device to an access group for assignment to identities and their tokens.

On the Panel: Status tab, the Credential Capacity count for the door is updated.

## Applying Door Commands

To control your Schlage IP wireless device, apply the following door commands:

1. Select **Physical Access** > **Doors**.
2. Enter a checkmark in the **All** column next to the device.
3. For the Control lock:
   - To grant access to the deadbolt on the Control lock, select **Door Action** > **Grant** (only this door action is supported). Momentarily grants access to the door to permit a single-time entry. Ignore the Unknown door state and door mode.

     The deadbolt is enabled for you to lock it (extend the bolt) or unlock it (retract the bolt) on the outside.
4. For the RU device:
   - To unlock the RU device in **Closed** door state and **Locked No Access** door mode, select **Door Action** > **Unlock** (only this door action and the Locked No Access door action are supported).

     The door mode changes to **Locked No Access (Unlocked on Next Exit)**. The door is locked on the outside and the inside. The remains displayed.

     When a person presses the push bar, the door is **Unlocked**. While the door is unlocked, you will see the **Open** and **Closed** states as the door is opened and closed.
   - To lock the RU device in **Closed** door state and **Unlocked** door mode, select **Door Action** > **Locked No Access**.

     The door is instantly locked.

For more information about controlling doors, see *Controlling Doors* on page 191. You can also apply door commands to RU devices in maps. For more information, see *Maps* on page 429.

## Door Scheduling By Batch Job (Specification)

To create a schedule for locking and unlocking doors, use a batch job specification. For more information, see *Scheduling Batch Jobs* on page 455 and *Setting Batch Door Modes* on page 461.

## Viewing Gateway or Offline Wi-Fi Lock Status

For IP/PoE mode and offline Wi-Fi mode ENGAGE gateways.

1. Select **Physical Access** > **Panels** to view gateways or offline Wi-Fi locks.
2. View the **Device Status** in the first column. For more information, see *Device Status* on page 43. Ignore the Cards in Use column.

   For another way of accessing device status, see *Using the Dashboard* on page 41.
3. Select the panel.
4. View on the **Status** tab:

| | |
|---|---|
| | The communications status between the panel and ACM appliance. The current status of the device is indicated by the background color. For more information, see *Status Colors* on page 43. |
| **Clock** | Resynchronizes the clock time of the gateway or offline Wi-Fi lock when clicked. See *Updating Panel Time* on page 172. |

| | |
|---|---|
| **Last comms** | The date and time of the last message that was communicated between the panel and the ACM appliance.<br>Offline Wi-Fi lock only. The date and time of the last communication between the lock and the ACM appliance. |
| **Next comms** | Offline Wi-Fi lock only. The date and time of the next communication between the lock and the ACM appliance. |
| **Firmware** | The gateway or offline Wi-Fi lock firmware version. See *Updating Schlage Gateway Firmware* on page 171.<br>**Note:** ControlBM locks are displayed in the **ControlBM Locks** list only if the gateway firmware is updated to version 1.62.04 or newer. If the gateway firmware is not updated, the ControlBM locks are displayed in the **Control Locks** list. Lock functionality still works with the exception of the **Update Firmware** capability.<br>Offline Wi-Fi lock only. Hover your mouse over the firmware version to view more details. |
| **Notes** | Add notes about the panel and review previous notes, if any. |

## Viewing Door Status and Events

To view access information, events and alarms generated for doors:

1. Select **Physical Access** > **Doors**.

   For more information about door state and door mode, see *Adding Doors* on page 214.

   For event descriptions, see *Troubleshooting* on page 490.
2. Select the name of the door.
3. Click the **Events** tab to view all the global events that are related to the device:

| | |
|---|---|
| **Name** | The name of the event. |
| **Event** | The type of event. |
| **Source Type** | The source of this event. |
| **Has On/Off** | If the event toggles on or off.<br>Click **Yes** or **No**. |
| **Masked** | If the event is masked.<br>Click to change status to (yes) or (no). |
| **Logged** | If the event is logged.<br>Click to change status to (yes) or (no). |
| **Show Video** | If a video is available for the event. If 'yes' is selected, the live video window automatically pops up when the event is received.<br>Click to change status to (yes) or (no). |

> **Tip:** You can also view events using **Monitor > Events**. For more information, see *Monitoring Events* on page 26.

4. Click the **Access** tab to view the access groups, roles and identities that have permission to edit or use the door (not applicable to RU and RM exit devices):

| | |
|---|---|
| **Access Groups** | The name of the access group. Click the link to edit the access group. |
| **Roles** | The roles that the access group is a member of. Click the + or - icon next to each role to show or hide the identities in the access group through the role. |
| **Identities** | The users who are members of the access group. |
| **Panel Date** | The date and time when the event occurred. |
| **Priority** | The priority of the event. The highest priority is 1 and the lowest priority is 999. |
| **Event** | The name of the event. |
| **Last Name** | The last name of the person who generated the event. |
| **First Name** | The first name of the person who generated the event. |
| **Card Number** | The internal token number assigned to the person who generated the event. |
| **Message** | Any messages that are associated with the event. |

For more information, see *Managing Door Access* on page 105.

5. Click the **Transactions** tab to view the events and alarms that have occurred at the door:

| | |
|---|---|
| **Access Groups** | The name of the access group. Click the link to edit the access group. |
| **Roles** | The roles that the access group is a member of. Click the + or - icon next to each role to show or hide the identities in the access group through the role. |
| **Identities** | The users who are members of the access group. |
| **Panel Date** | The date and time when the event occurred. |
| **Priority** | The priority of the event. The highest priority is 1 and the lowest priority is 999. |
| **Event** | The name of the event. |
| **Last Name** | The last name of the person who generated the event. |
| **First Name** | The first name of the person who generated the event. |
| **Card Number** | The internal token number assigned to the person who generated the event. |
| **Message** | Any messages that are associated with the event. |

For more information, see *Configuring Roles* on page 82.

# Updating Gateway and Offline Wi-Fi Lock Firmware

For Schalge IP wireless locks and offline Wi-Fi locks.

> **Note:** Ensure the ENGAGE gateway and ACM have access to the internet.

To apply firmware updates from lock manufacturers:

1. On the Panels  list, select the gateway.
2. For the device type, click **Update Firmware**. Ignore the blue Firmware button, which is used for updating gateway firmware.

   **Note:** To update the firmware of ControlBM locks, gateway firmware version 1.62.04 or newer, is required.

3. Do one of the following:
   - Click ✔ next to the firmware version that is available in the system to apply it to the group of locks.
   - Select a new firmware version as follows:
     a. Click **Open Advanced Options**.
     b. Enter your ENGAGE login information in **ENGAGE User** and **ENGAGE Password**, and click **Get Available Firmware**. The firmware versions are downloaded.

        **CAUTION —** This advanced procedure must be performed only by qualified personnel with the requisite knowledge of the firmware versions and the ACM system.

     c. Click ✔ next to the firmware file to apply it.

**Note:** For offline Wi-Fi locks, the firmware version update does not occur immediately. It occurs at the next communication interval to the ACM application. Each offline Wi-Fi lock has its own interval setting which is dependent on the timing of its initial communication with the ACM system.

## Generating Reports

For Schlage IP wireless devices.

You can generate the Door Configuration Report and Transaction Report by selecting **Reports**.

# Offline Wi-Fi Mode Installation

Add a Schlage ENGAGE™ site in ACM to configure and manage groups of Allegion Schlage® Wi-Fi locks. For more information, see:


- *Supported Devices* on the next page
- *Step 1: Creating an ENGAGE Site* on the next page
- *Step 2: Setting Up Communication to Offline Wi-Fi Locks* on page 277
- *Step 3: Configuring Offline Wi-Fi Lock Operation* on page 278


**Note:** ACM supports only the Schalge devices in *Supported Devices* on the next page in offline Wi-Fi mode. Other device models might not operate correctly.

**Note:** ACM appliance failover is not supported for offline Wi-Fi locks due to the connection method. Offline Wi-Fi locks initiate calls to the ACM appliance, as opposed to the ACM appliance initiating the connection for wired locks. However, manual failover to a standby ACM appliance is supported. To enable automated failover for offline Wi-Fi locks, organizations may choose to follow standard practices for network DNS failover in their infrastructure. The details of configuring automated failover depend on individual network architectures.

## Supported Devices

Ensure the physical configuration of the device matches the configuration in the ACM application as follows.

| Door<br><br>Linked Device | Panel | Subpanel | External System |
|---|---|---|---|
| *Allegion Schlage LE and NDE series* | | | |
| Up to 2048 wireless locks, depending on the ACM appliance or license — LE model | Same as doors | - | ENGAGE site |
| Up to 2048 mobile-enabled wireless locks, depending on the ACM appliance or license — LE version B (LEB ) and NDE version B (NDEB) models<br><br>Mobile credentials are not supported. | Same as doors | - | ENGAGE site |

## Step 1: Creating an ENGAGE Site

**Note:** Before you begin, obtain the ENGAGE login account information. For more information, see Schlage documentation.

To create an ENGAGE site in ACM:

1. Select >**External Systems**.
2. Click the **Schlage** tab.
3. Click the **Add Schalge Site** button.
4. Enter:

| | |
|---|---|
| **Site Name** | Up to 50 alphanumeric characters for the name of the site which represents the logical group of ENGAGE devices.<br><br>**Note:** Always create an ENGAGE site in the ACM application. A site that is already created in the ENGAGE application cannot be reused in the ACM application. In addition, a site cannot be used by more than one ACM appliance. |
| **ENGAGE User** | The login name of the ENGAGE account. |
| **ENGAGE Password** | The password of the ENGAGE account. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |

5. Click to save your changes.

   Click to discard your changes.

After you add the ENGAGE site for an IP-connected lock, see *Step 2: Configuring Gateways for IP-enabled Wireless Locks* on page 268.

After you add the ENGAGE site for an offline Wi-Fi lock, see *Step 2: Setting Up Communication to Offline Wi-Fi Locks* below.

## Step 2: Setting Up Communication to Offline Wi-Fi Locks

To set up communication between the offline Wi-Fi locks and the ACM appliance:

1. On the External Systems page, click the **Schlage** tab and enter:

| | |
|---|---|
| **Site for Schlage WiFi Locks** | The ENGAGE site that ACM will use to establish secure communication with the offline Wi-Fi lock when the lock attempts connection to ACM for the first time. |
| **Schlage WiFi Door Communication Interval** | The time interval for communication of the offline Wi-Fi lock to the ACM system. Default is 1440 minutes (24 hours). |
| **CA Certificate** | If you installed a custom certificate on your appliance, you need to upload the certificate of the Certification Authority that signed it. Click Upload CA Certificate to upload the certificate to ACM. Click to delete it.<br><br>You cannot edit this field if the appliance is using a default self signed certificate. |

2. Click to save your changes.
3. In the ENGAGE application, enter the ENGAGE site defined in the field above and the IP address of the ACM server. For more information, see vendor documentation.

After a lock is externally commissioned, the lock automatically appears in the ACM application as a door and

a panel.

> **Note:** ENGAGE uses port 443 to communicate with ACM. Make sure the ACM **Web Server Port** is set to 443 so the lock can successfully communicate with ACM. For more information, see *Appliance Fields - Appliance tab* on page 1.

After this step, see *Step 3: Configuring Offline Wi-Fi Lock Operation* below.

See also:

- *Deleting Offline Wi-Fi Locks* on page 280

## Step 3: Configuring Offline Wi-Fi Lock Operation

To configure lock operation:

1. Edit device settings as required:

   (The **Name** through **Installed** fields can be edited on the Parameters, Operations and Cameras tabs. For these field descriptions, see *Adding Doors* on page 214.)

   On the **Operations** tab, select:

| | |
|---|---|
| **Standard Access Time** | The seconds the door remains unlocked after access has been granted. |
| **Held Open Time** | The seconds the door can be held open before a Door Held Open event is generated. |
| **Extended Access** | The seconds the door remains unlocked after access has been granted to token holders with extended access permissions. |
| **Card Formats** | **Important:** To maximize the security and capacity of your locks, only move the card formats that are actually used to the **Members** column.<br><br>Make sure the **Facility Code** in Physical Access > Card Formats matches the facility code on the card. This ensures credential matching occurs during card operation on the door that uses the card format. For more information, see *Configuring Card Formats* on page 305.<br><br>**Note:** The **Suppress facility check** checkbox must not be used. |

2. Click ✔ to save your changes.

   Allow time for the device configuration to take effect.

   > **Important:** Check the credential capacity of the door on the Panel: Status tab before you add more credentials to the lock.

On the Panel: Status tab, the Credential Capacity count for the door is updated.

## Viewing Gateway or Offline Wi-Fi Lock Status

For IP/PoE mode and offline Wi-Fi mode ENGAGE gateways.

1. Select **Physical Access** > **Panels** to view gateways or offline Wi-Fi locks.
2. View the **Device Status** in the first column. For more information, see *Device Status* on page 43. Ignore the Cards in Use column.

   For another way of accessing device status, see *Using the Dashboard* on page 41.
3. Select the panel.
4. View on the **Status** tab:

| | |
|---|---|
| | The communications status between the panel and ACM appliance. The current status of the device is indicated by the background color. For more information, see *Status Colors* on page 43. |
| **Clock** | Resynchronizes the clock time of the gateway or offline Wi-Fi lock when clicked. See *Updating Panel Time* on page 172. |
| **Last comms** | The date and time of the last message that was communicated between the panel and the ACM appliance.<br>Offline Wi-Fi lock only. The date and time of the last communication between the lock and the ACM appliance. |
| **Next comms** | Offline Wi-Fi lock only. The date and time of the next communication between the lock and the ACM appliance. |
| **Firmware** | The gateway or offline Wi-Fi lock firmware version. See *Updating Schlage Gateway Firmware* on page 171.<br>**Note:** ControlBM locks are displayed in the **ControlBM Locks** list only if the gateway firmware is updated to version 1.62.04 or newer. If the gateway firmware is not updated, the ControlBM locks are displayed in the **Control Locks** list. Lock functionality still works with the exception of the **Update Firmware** capability.<br>Offline Wi-Fi lock only. Hover your mouse over the firmware version to view more details. |
| **Notes** | Add notes about the panel and review previous notes, if any. |

## Updating Lock Firmware

For Schalge IP wireless locks and offline Wi-Fi locks.

**Note:** Ensure the ENGAGE gateway and ACM have access to the internet.

To apply firmware updates from lock manufacturers:

1. On the Panels  list, select the gateway.
2. For the device type, click **Update Firmware**. Ignore the blue Firmware button, which is used for updating gateway firmware.

   **Note:** To update the firmware of ControlBM locks, gateway firmware version 1.62.04 or newer, is required.

3. Do one of the following:
   - Click ✔ next to the firmware version that is available in the system to apply it to the group of locks.
   - Select a new firmware version as follows:
     a. Click **Open Advanced Options**.
     b. Enter your ENGAGE login information in **ENGAGE User** and **ENGAGE Password**, and click **Get Available Firmware**. The firmware versions are downloaded.

        **CAUTION —** This advanced procedure must be performed only by qualified personnel with the requisite knowledge of the firmware versions and the ACM system.

     c. Click ✔ next to the firmware file to apply it.

**Note:** For offline Wi-Fi locks, the firmware version update does not occur immediately. It occurs at the next communication interval to the ACM application. Each offline Wi-Fi lock has its own interval setting which is dependent on the timing of its initial communication with the ACM system.

## Deleting Offline Wi-Fi Locks

To delete an offline Wi-Fi lock from the ACM application:

1. Uninstall the physical lock hardware.
2. Delete the door in the ACM application. For more information, see *Deleting Doors* on page 202.

   Deleting the door automatically deletes the associated panel.

If a lock is deleted in the ACM application, it will reappear as a new door at the next communication interval to the ACM application. A lock that is not deleted in the ACM application, but deleted in the ENGAGE application, will appear as an offline lock in the ACM application. Changing the site must be done in the ENGAGE application.

# SALTO Door Installation

Add a SALTO ProAccess SPACE server (referred to as SALTO server) in the ACM application to manage users and physical access to installed doors that are configured in the SALTO network. For more information, see:


- *System Overview* below
- *Prerequisites* on the next page
- *Supported Devices* on page 285
- *Step 1: Connecting to a SALTO Server* on page 285
- *Step 2: Configuring the SALTO Server* on page 286
- *Step 3: Syncing Doors with the SALTO Server* on page 286
- *Step 4: Installing and Configuring Doors* on page 287
- *Step 5: Creating Identities and Tokens* on page 288


**Note:** Doors must be created in the SALTO system before you use the ACM system. Every time you add or delete doors in the SALTO system, remember to manually sync them with ACM as described in Step 3. In addition, identities and their tokens must be managed in the ACM system and requires using encoder hardware for some door modes, as described in Step 5.

## System Overview

**Figure 5:** ACM system organization for SALTO ProAccess SPACE doors

| | |
|---|---|
| 1 | ACM applications, including identity (badging), administration, video surveillance and alarm monitoring |
| 2 | ACM appliance |
| 3 | Encrypted connection provided by the SALTO Host Interface Protocol (SHIP) integration |
| 4 | SALTO ProAccess SPACE server (referred to as SALTO server; supports up to 2048 installed doors), SALTO ProAccess SPACE Configurator application, SALTO encoder hardware<br>**Note:** Installing the SALTO ProAccess SPACE server on a dedicated machine is recommended for the best performance. |
| 5 | SALTO network |
| 6 | SALTO JustIN Mobile access technology and mobile credentials, physical keycards |

# Prerequisites

## SALTO Server Installation and Configuration

Contact your integrator to install and configure the SALTO ProAccess SPACE server.

> **Note:** Operators need to understand how to use SALTO security configuration, such as key revalidation, door open mode and timed-based configuration, before using the ACM system. See *Understanding SALTO and ACM Door Configuration* on the next page.
>
> For general, new or updated instructions about the registration, installation and configuration of SALTO systems software and hardware, refer to SALTO systems documentation. The following instructions are based on using SALTO ProAccess SPACE software version 6.6.2.4 or newer.

1. In the SALTO ProAccess SPACE Configurator application, set up the encrypted connection:
   a. If the ProAccess SPACE service is running, select the **SERVICE PROPERTIES** panel and stop it.
   b. Select the **SERVICE PORTS** panel.
   c. Select **SALTO authentication** and enter the port used for communication between SALTO and ACM systems. Default is 8100.

      This is the same port used in the URL to access the SALTO ProAccess SPACE web interface.
   d. Select the **Use HTTPS** checkbox and then select the required certificate from the dropdown list.

      If your certificate is not listed, make sure the certificate and its private key are stored in a .pfx file and then imported to the Windows certificate store.

      > **Note:** The above steps assume you are running Windows 10. If you are running Windows 7 Service Pack (SP) 1, upgrading to Windows 10 or enabling Transport Layer Security (TLS) in Windows 7 SP 1 is recommended. For more information, see the steps at Microsoft.com (support.microsoft.com/en-ca/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi).
   e. Select the **DATABASE** panel and select **Windows authentication**.
   f. Save the settings.
   g. Start ProAccess SPACE service.
2. On your Windows machine, ensure the firewall can support inbound and outbound traffic on the port used for communication between SALTO and ACM systems.
3. In the SALTO ProAccess SPACE software version 6.6.2.4 or newer, configure the user ID:
   a. Click the URL which is displayed on the **SERVICE PORTS** panel.

      For example: `https://hostname:portnumber/ProAccessSpace/`
   b. Select the **Advanced** tab on **General options**.
   c. Add the **SHOW_EXT_ID** parameter and set the value to **1**.

d. Select the **Users** tab and click the button next to **User ID configuration**.
e. Add **($FirstName) ($LastName) ($EXTID)** in the **Content** field and click **OK**.

> **Important:** The ($EXTID) macro must be used to ensure uniqueness of the First Name and Last Name combination.

4. In the SALTO ProAccess SPACE software, configure the SHIP integration:
   a. Select **System** > **General options** from the menu bar.
   b. Select the **SHIP** tab on **General options**.
   c. Click the **Enable** checkbox.
   d. Click **HTTP(S)** and select **Basic** from **Authentication**.
   e. Create a username and password to connect with the ACM system.
   f. Save the settings.

## Understanding SALTO and ACM Door Configuration

When you install doors in the SALTO system, consider the following:

- SALTO door open mode configuration is mapped to the ACM Door mode and Custom Mode fields.

  Creating, updating or removing an open door mode in the SALTO system will add, update or remove (respectively) the mapped field values in the ACM system *after a manual sync in ACM*. See the following table for the field values. When doors are deleted in the ACM system, the corresponding doors in the SALTO system are not deleted. At the next manual sync in the ACM system, the door will display as a new uninstalled door.
- SALTO Timed period field is mapped to the ACM Custom Schedule field.

  Creating, updating or removing a schedule that is assigned to a door in the ACM system will create, update or remove (respectively) the Timed period value in the SALTO system.
- SALTO calendar group configuration is mapped to ACM holiday configuration.

  Creating, updating or removing a holiday in the ACM system will add, update or remove (respectively) the calendar and any holidays in the SALTO system.

For information about ACM door configuration, see *Door Modes* on page 203, *Step 3: Syncing Doors with the SALTO Server* on page 286 and *Step 4: Installing and Configuring Doors* on page 287.

For information about SALTO door configuration, refer to SALTO systems documentation.

| ACM System | | SALTO System |
|---|---|---|
| **Door Mode** | **Custom Mode** | **Door Open Mode** |
| Card Only | - | Standard |
| | Unlocked | Automatic opening |
| | Card and PIN | Timed Key + PIN |
| | Office | Timed office |
| | Toggle | Timed toggle |
| | Keypad Only | Timed keypad |
| Card and Pin | - | Key + PIN |
| Office | - | Office |
| | Unlocked | Automatic opening + Office |
| Toggle | - | Toggle |
| | Unlocked | Automatic opening + Toggle |
| Keypad Only | - | Keypad only |
| Exit Leaves Open‡ | - | Exit Leaves Open‡ |
| Toggle and Exit Leaves Open‡ | - | Toggle and Exit Leaves Open‡ |
| - | - | Another door mode |

| **Custom Schedule** | **Timed Period*** |
|---|---|
| Up to 1024 schedules | 1024 timed periods |

| **Holiday** | **Calendar*** |
|---|---|
| Up to 3 types of holiday groups | In calendar name (0000), 1 holiday and 2 special holidays |

‡ The Escape and Return mode settings are not applicable to SALTO online and standalone doors that are installed with a control unit (CU).

***Escape and Return Mode***

In the SALTO ProAccess SPACE software version 6.6.2.4 or newer, configure the lock mode:

1. Select **System** > **General options** > **Advanced**.
2. Add the **EXIT_LEAVES_OPEN** parameter and set the value to **1**.
3. Save the setting.

**Note:** You can search for Escape and Return events in ACM event monitoring.

### SALTO Ethernet Encoder Configuration

In the SALTO ProAccess SPACE software version 6.6.2.4 or newer, configure the encoder:

1. Go to **SALTO Network** and click the **Add Network Device** button.
    a. Select **Encoder** and click **OK**.
    b. Enter the **Name** and **Description**, and **IP address** for Ethernet access.
    c. Save the setting.
    d. Verify the encoder is online.
        i. Press the LED button at the back of the physical device until it flashes.
        ii. Click the **Address** button to initiate the connection.
        iii. Click the **Status Monitoring** button.
2. Select the operator login in the upper-right corner.
    a. Select **Settings** > **Local Settings** > **Encoder Settings**.
    b. Select **Online** and the encoder name.
    c. Save the setting.

For more information about SALTO Ethernet encoder configuration, refer to SALTO systems documentation.

## Supported Devices

The ACM application is mapped to the physical configuration of SALTO doors as follows.

| Door | Panel | Subpanel | External System |
|---|---|---|---|
| Up to 2048 installed doors<br><br>All SALTO door devices at time of initial release in ACM | A SALTO server is a panel. | - | A SALTO server is a panel. |

## Step 1: Connecting to a SALTO Server

**Note:** Before you begin, set up the required SALTO server and hardware. For more information, see SALTO systems documentation.

**Important:** Only one ACM system can connect to a SALTO server. Connecting more than one ACM system is not supported.

To connect to a SALTO server in ACM:

1. Select > **External Systems**.
2. Click the **SALTO** tab.
3. Enter:

| | |
|---|---|
| **Appliance** | The name of the ACM appliance that is connected to the SALTO server. |
| **Address** | The IP address or hostname of the SALTO server. |
| **Port** | The TCP/IP port number configured on the SALTO server. |
| **User Name** | The SALTO user name created in the SHIP encryption step in *Prerequisites* on page 282. |
| **Password** | The password for the user name. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Installed** | Enables communication between the ACM appliance and server after saving. |

4. Click the **Create** button.

After the external system is saved, the SALTO server automatically appears in the ACM application as a panel.

## Step 2: Configuring the SALTO Server

To configure the new SALTO server:

1. Select **Physical Access>Panels**.
2. Select the SALTO panel.
3. Click the **Configure** tab on the SALTO panel.
4. Enter:

| | |
|---|---|
| **Physical Location** | A description of where the device is installed. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |

The other fields are read-only and cannot be changed. For more information, see *SALTO Panel Configuration* on page 168.

5. Click to save your changes.

After saving the panel, see *Step 3: Syncing Doors with the SALTO Server* below.

## Step 3: Syncing Doors with the SALTO Server

To import SALTO doors to the ACM appliance:

- On the **Status** tab of the SALTO panel, click **Sync Doors**.

  Doors are imported uninstalled. Sync Status displays the sync results. Doors in a zone in the SALTO system are displayed as doors in the ACM system.

> **Note:** Every time you add or delete doors in the SALTO system, remember to sync them with the ACM system.

The other fields are read-only and cannot be changed. For more information, see *SALTO Panel Status* on page 168.

After doors are imported, see *Step 4: Installing and Configuring Doors* below.

## Step 4: Installing and Configuring Doors

> **Note:** Doors must be created in the SALTO system before you use Door Mode, Custom Mode and Custom Schedule in the ACM system.

To enable communication to the SALTO door after syncing with the SALTO server:

1. Select **Physical Access** > **Doors**.
2. Install the door to enable communication with ACM, if not already done:
   a. Select the door displaying the device status.
   b. Select **Installed** > **Install**.
   c. Click **OK**.

> **Note:** If a message (red text) is displayed indicating the need to update the door mode, make sure the Door Mode, Custom Mode and Custom Schedule fields are selected. You need to set supported door modes in the ACM appliance.
>
> If you add a door to a zone or remove a door from a zone in the SALTO system, allow up to five minutes for the door to be added or deleted (respectively) in the ACM system.

3. Display the event details for each door in the list, if not already done:
   a. Select the door name.
   b. On the **Parameters** tab, enter a checkmark in **Detailed events**.
   c. Click to save.
4. Return to **Physical Access** > **Doors**.
   - In the **Device Status** column, you will see:

     *Online with control unit door.* Normal, Uninstalled, Communication, Unlocked, Battery, Tamper, Forced, Held or Synchronization.

     *Standalone door.* Normal, Uninstalled, Battery or Synchronization.

     For more information, see *Device Status* on page 43.
   - In the **Door State** column, you will see Unknown change to:

*Online door.* Open, Closed, Emergency Open or Emergency Closed.

*Standalone door.* Offline.

*Online or standalone door with no control unit*. Closed or Emergency Open.

For more information, see *Controlling Doors* on page 191 and *Maps* on page 429.

- In the **Door Mode** column, you will see:

  *Online and standalone doors.* Card Only, Card and Pin, Toggle, Office or Keypad Only.

  *Online or standalone door with no control unit*. Unlocked or Locked No Access.

  For more information, see *Door Modes* on page 203.

5. Select and edit door configuration as required:

   (The **Alt Name** through **Installed** fields can be edited on the Parameters and Cameras tabs. For these field descriptions, see *Adding Doors* on page 214.)

   **Door Mode**: The entry mode of the door after syncing with the SALTO server and installing the door. For more information, see *Door Modes* on page 203.

   **Custom Mode**: Another entry mode of the door that is time-based (see Custom Schedule), which can be **Unlocked**, **Card and Pin**, **Office**, **Toggle** or **Keypad Only** (same as Door Mode). If Keypad Only is selected, **Keypad Code** is displayed. You can enter up to 8 digits.

   **Custom Schedule**: A predefined time when Custom Mode becomes active. If you need to add a new schedule, see *Adding Schedules (Intervals in Schedules)* on page 377.

   **Always Mask Forced**: If selected, Door Forced Open alarms at the door are always masked.

   **Always Mask Held**: If selected, Door Held Open alarms at the door are always masked.

   **Detailed events**: Enables the reporting of event details, such as Door Mode, after syncing and installing the door.

   **Do Not Log Rex Transactions**: Disables logging of request-to-exit transactions.

6. Click ✔ to save your changes.

See *Step 5: Creating Identities and Tokens* below.

- *System Overview* on page 281

## Step 5: Creating Identities and Tokens

**Note:** Before you start, make sure you have access to encoder hardware before you create the identity and token in the ACM system. In addition, make sure an access group and identity are created in the ACM system. For more information, see *Adding an Access Group* on page 105 and *Assigning an Access Group to a Role* on page 107.

If your SALTO network supports SALTO mobile credentials, make sure all identities download and install the SALTO JustIN Mobile app.

To create an identity and token for a SALTO door:

1. Select **Identities** > **Identities** and click **Search** to select an identity already created.

   If you need to add an identity, see *Adding an Identity* on page 65.

2. Click the **Tokens** tab and enter:

| Token Type | SALTO |
|---|---|
| **Mobile Application Type** | Default is **None**.<br>**JustIn Mobile** refers to the SALTO JustIN Mobile application that is installed on the mobile phone of the identity.<br>**Note:** When issuing mobile keys, the encoder requires access to the internet. |
| **Mobile Phone Number** | The mobile phone number in international format (plus sign and no spaces).<br>+ country code, area code, phone number<br>Example: `+12345678910`<br>**Note:** The mobile app must be installed on the mobile phone of this phone number. |

   For other field descriptions, see *Token Fields* on page 76.

3. Click ✔ to save.

   The **Download** and **Assign Key** buttons appear.

4. Edit the token and click **Assign Key** to assign a key to the token as follows:

   *For a physical key:*

   a. Select the SALTO encoder in the dialog box and click **Next**.
   b. *SALTO encoder step*. Place the physical key on the encoder hardware.
   c. Click the **Encode Key** button in ACM.
   d. Click **OK**.

   *For a mobile key:*

   - Click **OK**.

   ACM displays the status of the key update.

## Using Physical and Mobile Keys

To use a physical key after assigning or editing a token:

- Place the keycard on the SALTO door device.

To use a mobile key after assigning or editing a token:

a. Tap the key icon in the mobile app.
b. Place the mobile phone on the SALTO door device for 1-2 seconds until a checkmark is displayed.

# Editing Tokens — Update Required and Re-edition Required

If the Update Required or Re-edition Required status (red box) appears on the Tokens tab, edit token configuration as follows:

> **Note:** Updating some of the token configuration requires you to re-encode (referred to as re-edition or re-edit) the key. Therefore, make sure you have access to encoder hardware before you start.

1. Select the token configuration:

| | |
|---|---|
| **PIN** | When a PIN is required, the PIN number that the user will be required to enter at a keypad card reader. |
| **Token Status** | The status of the token may be set manually and then updated by the system as follows:<br>• **Active**: The Not Yet Active token is set to Active when the current date is past the Activate Date.<br>• **Expired**: The Active token is set to Expired when the current date is past the Deactivate Date.<br>• **Inactive**: The Active token is set manually to Inactive without further update.<br>• **Not Yet Active**: The token is not active yet. |
| **Issue Level** | A number from 0 to 999999999, representing the issue level of the token.<br>Example: If a 3-digit length was configured on the Card Format: Edit page, you can enter 123 for the issue level of the card.<br>For more information, see *Issue Level Numbering for Reusing a Card Number* on page 307. |
| **Never Expire** | The token never expires. |
| **Extended Door Times** | A checkbox to give the token extended access time.<br>Once enabled, the door remains unlocked for a longer period of time than the standard access time to accommodate users that may require more time to enter a door.<br>Standard and extended access times are specified on the Door Edit page. |
| **Office** | A checkbox to enable the token to activate Office mode for a door that is configured for Office mode, which allows the cardholder to leave the lock open.<br>To use this mode, the cardholder presents the key to the door while pressing down the inner handle and repeats the procedure to undo the mode. |
| **Set Lockdown** | *SALTO standalone doors only.* A checkbox to enable lockdown mode for a door that has a lock that can support manual lockdown. For more information about lockdown in the SALTO system, refer to SALTO systems documentation.<br>To use this mode, the cardholder presents the key to the door's inside reader and repeats the procedure to undo the mode. |

| | |
|---|---|
| **Override Privacy** | A checkbox to allow the cardholder to access a door locked from the inside at any time. |
| **Override Lockdown** | A checkbox to allow the person to access a door closed from the inside during lockdown state. |
| **Audit Openings** | *SALTO standalone doors only.* A checkbox to audit the use of keys in standalone doors. Audits automatically occur in online doors. |
| **Enable Revalidation**<br>**Update Period** in **days** or **hours** unit | A checkbox to specify a period for revalidating a key before it becomes invalid. To make the token valid again, the cardholder can present the token to the online wall reader at any time.<br>For example, a key requires revalidation every seven days, if the update period is set to 7 days. If the key is used on the third day, the update period is reset. If the key is not used for over seven days, the key becomes invalid.<br>**Note:** When revalidating mobile keys, the encoder requires access to the internet. |
| **Issue Date** | The date the token was issued. |
| **Activate Date** | The activation date for the token. |
| **Deactivate Date** | The deactivation date for the token. |
| **Last Door** | The last door the token was used to gain access. |
| **Last Used** | The last time the token was used to gain access. |

2. Click the **Update Key** button in ACM.
3. If updating **Audit Openings**, **Override Privacy** or **Override Lockdown**:

   *For a physical key:*

   a. Select the SALTO encoder in the dialog box and click **Next**.
   b. *SALTO encoder step.* Place the physical key on the encoder hardware.
   c. Click the **Encode Key** button in ACM.
   d. Click **OK**.

   *For a mobile key:*

   - Click **OK**.

   ACM displays the status of the key update, such as the No Update Required status.

## Canceling Keys

To cancel a key that was assigned to a token:

1. On the **Tokens** tab, click the **Cancel Key** button.

   ACM displays the status of key update.
2. Click **OK** .

**Note:** A canceled key cannot be used throughout the SALTO system. For more information, refer to SALTO system documentation.

## Downloading All Tokens

To download or restore all tokens to the ASSA ABLOY, HID or Mercury panel:

- On the **Status** tab of the panel, click **Tokens**.

Typically, this action is done after system restore. For more information, see also *Restoring Backups* on page 351.

# ASSA ABLOY™ IP-enabled Lock Installation

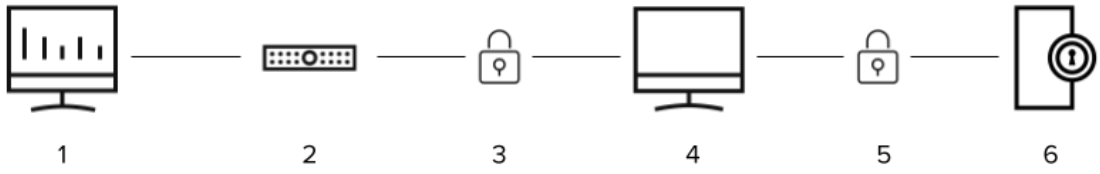
Add a panel in ACM to configure and manage groups of ASSA ABLOY IP-enabled locks, including hard-powered PoE (Power over Ethernet) locks and battery-powered Wi-Fi locks, after their initial configuration and connection to the Door Service Router (DSR) server (referred to as DSR). Typically, Wi-Fi locks are battery-powered (referred to as the Battery Powered lock type), and if configured with an external power supply, can have the real-time communication capabilities of hard-powered PoE locks (referred to as the External Powered lock type). For more information, see:


- *System Overview* below
- *Prerequisites* on the next page
- *Supported Devices* on page 295
- *Step 1: Configuring a Door Service Router for IP-enabled Locks* on page 295
- *Step 2: Syncing Doors with the Door Service Router* on page 296
- *Step 3: Installing and Configuring Doors* on page 297
- *Step 4: Configuring Locking Operation* on page 298


**Note:** Locks must be created in the Lock Configuration Tool (LCT) and doors must be created in the DSR software before you use the ACM system. Every time you add doors in the ASSA ABLOY system, remember to manually sync them with ACM as described in Step 2. After door sync, the doors must be edited and managed in the ACM system.

## System Overview

**Figure 6:** ACM system organization for ASSA ABLOY IP-enabled locks




| | |
|---|---|
| 1 | ACM applications, including identity (badging), administration, video surveillance and alarm monitoring |
| 2 | ACM appliance |
| 3 | Encrypted connection provided by the ACM appliance certificate and ASSA ABLOY DSR server configuration using Transport Layer Security (TLS) |
| 4 | ASSA ABLOY Door Service Router server, DSR Support Tool and Lock Configuration Tool applications |
| 5 | Encrypted connection provided by LCT network configuration |

6 ASSA ABLOY IP-enabled external powered (hard powered) PoE locks and battery-powered Wi-Fi locks

Typically, Wi-Fi locks are battery-powered (referred to as the Battery Powered lock type in ACM), and if configured with an external power supply, can have the real-time communication capabilities of hard-powered PoE locks (referred to as the External Powered lock type in ACM).

## Prerequisites

Contact your integrator to install and configure the ASSA ABLOY DSR software and LCT application.

**Note:** Integrators can download the required vendor software in the Avigilon Partner Portal (avigilon.com/software-downloads) and refer to the *Access Control Manager™ System Integration Guide for ASSA ABLOY Door Service Router and Lock Configuration Tool* (avigilon.com/products/access-control/wireless-lock-integrations#downloads).

## Supported Devices

The ACM application is mapped to the physical configuration of ASSA ABLOY IP locks as follows.

| Door | Panel | Subpanel | External System |
|---|---|---|---|
| Up to 1024 doors to a single DSR<br><br>Up to 2048 doors combined to two DSRs<br><br>DSR version 8.0.13 — Including SARGENT Profile Series v.S2, SARGENT Passport 1000 P2, SARGENT IN120 WiFi, CORBIN RUSSWIN IN120 WiFi, CORBIN RUSSWIN Access 700 PWI1 WiFi, CORBIN RUSSWIN Access 800 PWI1WiFi locks<br><br>Credentials are dependent on lock model. See vendor documentation for the limit. | A DSR is a panel. | - | - |

## Step 1: Configuring a Door Service Router for IP-enabled Locks

**Note:** Before you begin, set up the required DSR and LCT software and IP lock hardware. For more information, see the *Access Control Manager™ System Integration Guide for* the *ASSA ABLOY Door Service Router and Lock Configuration Tool*. For information about the number of DSRs supported by the ACM system, see *Supported Devices* above.

**Important:** The encrypted connection to the ACM system must be enabled in the DSR software.

To configure a DSR in ACM:

1. Select **Physical Access > Panels**.
2. Click **Add Panel**.
3. Enter:

| | |
|---|---|
| **Name** | A unique name for the panel. Choose a name that will help you identify the devices it controls. Duplicate names are not allowed. |
| **Physical Location** | A description of where the device is installed. |
| **Appliance** | The name of the ACM appliance that is connected to the DSR. |
| **Vendor** | **ASSA ABLOY** |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Installed** | Enables communication between the ACM appliance and installed device after saving. |
| **Model** | The model of the DSR. |
| **Timezone** | The local time which the panel operates in for door schedules and other time-based configuration. |

4. Click to save your changes. The entries are displayed on the **Configure** tab.

   (The **Name** and **Physical Location** fields can be edited on the Configure and Host tabs. The other fields are read-only and cannot be changed.)
5. Click the **Host** tab.
6. Enter:

| | |
|---|---|
| **IP Address** | The IP address of the gateway or hostname of the device. |
| **Access Port** | The remote port on the DSR that ACM sends commands to. Default is 8443 which must match the DSR setting. |
| **Callback Port** | The ACM port that receives events and status callback messages from the DSR. Default is 9000 for DSR1, 9001 for DSR2, and so on. Supported range is 0-65535.<br><br>**Note:** The callback port must be unique for each DSR, if you are installing multiple DSRs on the same ACM appliance. |

7. Click to save your changes.

After configuring the panel, see *Step 2: Syncing Doors with the Door Service Router* below.

## Step 2: Syncing Doors with the Door Service Router

To sync ASSA ABLOY IP doors with the ACM appliance:

- On the **Status** tab of the ASSA ABLOY panel, click **Sync Doors**.

  Doors are imported uninstalled. Sync Status displays the sync results.

  **Note:** Every time you add doors in the DSR software, remember to sync them with the ACM

system.

After doors are synced, see *Step 3: Installing and Configuring Doors* below.

## Step 3: Installing and Configuring Doors

**Note:** Doors must be created in the ASSA ABLOY system before you use Door Mode, Custom Mode and Custom Schedule in the ACM system.

To enable communication to the ASSA ABLOY door after syncing with the DSR:

1. Select **Physical Access** > **Doors**.
2. Install the door to enable communication with ACM, if not already done:
   a. Select the door displaying the device status.
   b. Select **Installed** > **Install**.
   c. Click **OK**.
3. Return to **Physical Access** > **Doors**. Door information is displayed in the following columns.

| | |
|---|---|
| **Device Status** | *For External Powered doors*, you will see Normal, Uninstalled, Communication, Unlocked, Battery, Tamper, Forced, Held or Synchronization.<br>*For Battery Powered door*, you will see Normal, Uninstalled, Battery or Synchronization.<br>For more information, see *Device Status* on page 43. |
| **Door State** | Unknown will change as follows.<br>*For External Powered doors*, you will see Open, Closed, Forced or Held.<br>*For Battery Powered doors*, you will see Normal or Offline.<br>For more information, see *Controlling Doors* on page 191 and *Using a Map* on page 432. |
| **Door Mode** | Unknown will not change for all listed doors. |

4. Select and edit door configuration as required:

   (The **Name** through **Installed** fields can be edited on the Parameters, Operations and Cameras tabs. For these field descriptions, see *Adding Doors* on page 214.)

| | |
|---|---|
| **Door Mode** | The entry mode of the door after syncing with the DSR and installing the door, which can be Unlocked, Card Only, Card and Pin, or First Person Through.<br>For more information, see *Door Modes* on page 203. |
| **Custom Mode** | Another entry mode of the door that is time-based (see Custom Schedule), which can be Unlocked, Card Only, Card and Pin, or First Person Through (same as Door Mode). |

| | |
|---|---|
| **Custom Schedule** | A predefined time when Custom Mode becomes active. If you need to add a new schedule, see *Adding Schedules (Intervals in Schedules)* on page 377.<br><br>**Tip:** If a message indicates the Advanced Schedule option cannot be enabled when saving, do any of the following:<br>• Save the schedule without Advanced Schedule selected. Some doors only support basic schedules.<br>• Find the access groups using the schedule and select another schedule. |
| **Lock Function** | None is the default. **Privacy**: When the interior lock button is pressed, the door will lock and the exterior lock will not grant access to any token. To unlock the door, the interior lock button must be pressed again or exit the room. |
| **Always Mask Forced** | If selected, Door Forced Open alarms at the door are always masked. |
| **Always Mask Held** | If selected, Door Held Open alarms at the door are always masked. |
| **Detailed events** | Enables the reporting of event details, such as Door Mode, after syncing and installing the door. |
| **Do Not Log Rex Transactions** | Disables logging of request-to-exit transactions. |

5. Click ✔ to save your changes.

See *Step 4: Configuring Locking Operation* below.

## Step 4: Configuring Locking Operation

To configure locking operation for the ASSA ABLOY IP door:

1. Edit device settings as required:

   (The **Name** through **Installed** fields can be edited on the Parameters, Operations and Cameras tabs. For field descriptions, see *Adding Doors* on page 214.)

   On the **Operations** tab, select:

| | |
|---|---|
| **Into Area** | The area that the badge holder enters by passing through the door.<br>Example: Laboratory<br>For more information, see *Adding Areas* on page 301. |
| **Out of area** | The area that the badge holder leaves by passing through the door.<br>Example: Lobby<br>For more information, see *Adding Areas* on page 301. |
| **Standard Access Time** | The seconds the door remains unlocked after access has been granted. |
| **Held Open Time** | The seconds the door can be held open before a Door Held Open event is generated. |

| | |
|---|---|
| **Extended Access** | The seconds the door remains unlocked after access has been granted to token holders with extended access permissions. |
| **Card Formats** | **Important:** To maximize the security and capacity of your locks, only move the card formats that are actually used to the **Members** column.<br><br>Make sure the **Facility Code** in Physical Access > Card Formats matches the facility code on the card. This ensures credential matching occurs during card operation on the door that uses the card format. For more information, see *Configuring Card Formats* on page 305. |

2. Click to save your changes.
   Allow time for the device configuration to take effect.

**Important:** Before you add more credentials to the lock, refer to the DSR software for the available credential capacity. Credential capacity is dependent on the lock model.

## Door Scheduling By Batch Job (Specification)

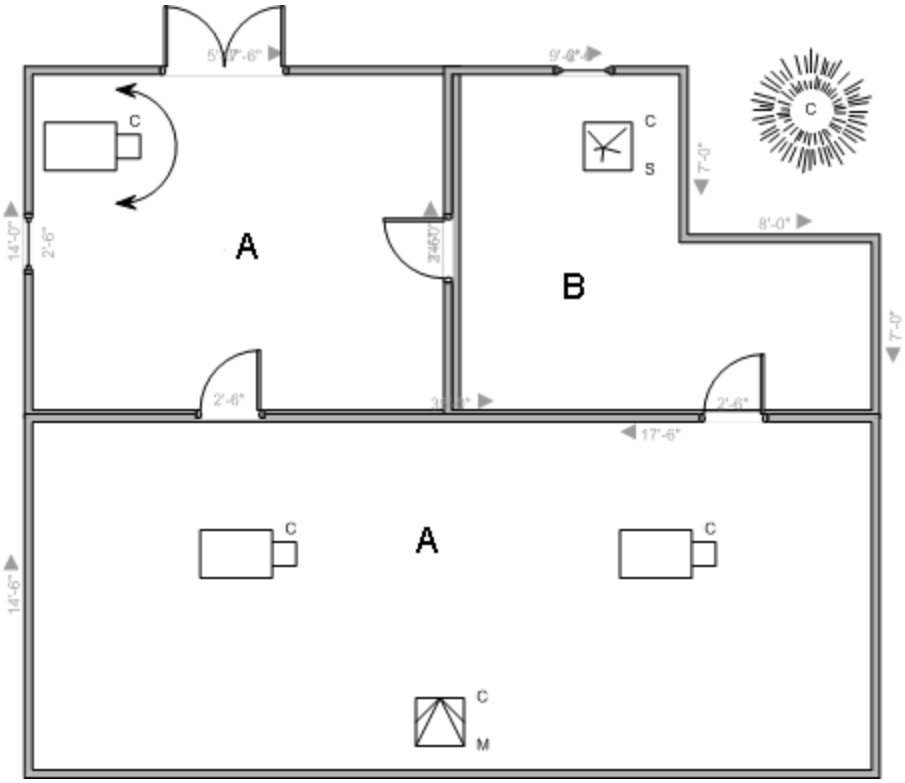
To create a schedule for locking and unlocking doors, use a batch job specification. For more information, see *Scheduling Batch Jobs* on page 455 and *Setting Batch Door Modes* on page 461.

# Configuring Areas

An area in the ACM system defines a physical location within a secured site that requires additional access control. This area can be relatively small, like a lab or a store room; or large, like a collection of buildings. Areas often incorporate one or more doors with their attached inputs and outputs. You can define areas to track badge holder location, for example in a mustering scenario, or to control access to specific areas, for example in an anti-passback configuration to limit user access within a building or facility.

**Note:** Do not confuse areas with partitions. A partition is a separate administrative access zone within the ACM system. An area is a physical location that requires additional access control. Therefore, in a partitioned system, an area is configured within a partition.

For example, an anti-passback configuration can be used in a laboratory facility to restrict access to a specific room.




The laboratory is divided into Area A and Area B. To secure Area B, only lab personnel who are permitted into both Area A and B can access the lab in Area B. To allow this, the doors are configured as follows:

- The door between the smaller room in Area A and Area B is configured as Out of Area A/Into Area B. It is the entry door for Area B.
- The door between the larger room in Area A and Area B is configured as Out of Area B/Into Area A. It is the exit door for Area B.
- The right-side of the double door when entering Area A is configured as an Into Area A door.
- The right-side of the double door when exiting Area A is configured as an Out of Area A door.

Lab personnel with permission to enter Area A are admitted through the right side of the double door when they swipe their entry card on the door reader. The ACM system records they are "Into Area A". Lab personnel with permission to enter Area A and Area B can then enter Area B at the door between the smaller room in Area A and Area B when they swipe their entry card on that door's reader. The ACM system records they are "Out of Area A" and "Into Area B". After they have entered Area B, they can exit from the other door to Area A. The ACM system records they are "Out of Area B" and "Into Area A". Lab personnel exiting Area A swipe their entry card on the reader on the right side of the double door. The ACM system records they are "Out of Area A".

Defined areas are added to the **Area into area** and **Area out of area** option list on the Doors Operations page. For more information, see *Configuring Doors* on page 189.

## Searching for an Area

You can search for areas by search criteria, such as name, enable area, 2-person control, or appliance.

1. Specify your **Search Field** in the drop down list.
2. Select any needed conditions from the **Search Value**drop down list to refine your search.
3. To add more search criteria, do the following, otherwise proceed to step 4:
    a. Click **Add Criteria**.
    b. Repeat steps 1 to 2.
    c. Select either:
        - **And** to find all items that fit all entered criteria.
        - **Or** to find items that fit one or more of the entered criteria.
    d. Continue adding search criteria as needed.
4. Click **Search**.
   The page displays your search results.

To clear all fields, click **Clear Search**.

To remove a search row, click **Remove**.

## Adding Areas

1. Select **Physical Access** > **Areas**.
2. From the Areas list, click **Add Area**.
3. Enter a name for the area.
4. Select the appliance that will maintain the area details.
5. Select the **Enable Area** checkbox to activate the new area.
6. Fill in the other options as required.
7. Click .
   The new area is added to the Area Listings page.

## Editing Areas

1. Select **Physical Access** > **Areas**.
2. Click the name of the area you want to edit.
3. On the following page, make the required changes.
   If you want to change the doors that are connected to the area, you must do so from the door's Operations page.
4. Click .

## Deleting Areas

1. Select **Physical Access** > **Areas**.
2. From the Areas list, click for the area you want to delete.
3. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.

# EOL Resistance

End-of-line (EOL) resistance refers to the resistance levels that must be maintained for input points. Input

devices used with doors often measure circuit resistance in ohms. This measurement is used to determine the normal resistance level. If the resistance drops across the circuit, an alarm is sent back to the ACM application.

For example, if resistance for a particular device has been set at 2000 ohms and the circuit's resistance suddenly drops to 1000 ohm, an alarm is issued by the application.

## Adding EOL Resistance for Mercury Input Points

To add an EOL Resistance definition for a Mercury input device:

1. Select **Physical Access** > **EOL Resistance**. Make sure the Mercury tab is selected.
2. From the Mercury EOL Resistance list, click **Add-Normal** or **Add-Advanced**.
3. On the following EOL Resistance Add page, enter the required details.
4. Click to save your changes.

## Adding EOL Resistance for VertX® Input Points

To add an EOL Resistance definition for an VertX® input point:

1. Select **Physical Access** > **EOL Resistance** > **HID**.
2. From the HID list, click **Add**.
3. Enter the required details.
4. Click to save your changes.

## Editing EOL Resistance for Mercury Input Points

To edit an EOL Resistance definition for a Mercury input device:

1. Select **Physical Access** > **EOL Resistance**. Make sure the Mercury tab is selected.
2. Select the EOL Resistance definition that you want to edit.
3. On the following page, make the required changes.
4. Click to save your changes.

## Editing EOL Resistance for VertX® Input Points

To edit an EOL Resistance definition for a VertX® input point:

1. Select **Physical Access** > **EOL Resistance** > **HID**.
2. On the HID list, select the EOL Resistance definition that you want to edit.
3. On the following page, make the required changes.
4. Click to save your changes.

# Mercury LED Modes - List page

The Mercury LED Modes list lists the available Mercury Security LED modes.

Select a mode from the list of custom LED modes to modify its settings. The *Mercury LED Mode Table*

*<number> page* is displayed. For more detail, see *Editing LED Modes* below.

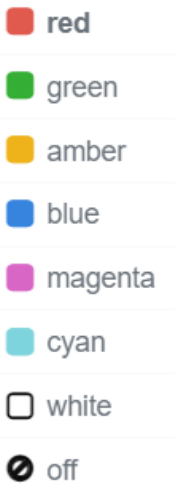
Before making any changes ensure that the related doors and subpanels are correctly configured and wired, including:

- Ensure that the **LED drive** field on the Reader: Edit screen has a valid entry (e.g. Gen 1 wire, Sep Red/Grn no buz, OSDP).
- Ensure that the **LED Mode** field on the Mercury Security Operations page is set to match the table (1, 2 or 3) that you want to use.

## Editing LED Modes

1. Select **Physical Access** > **Mercury LED Modes**.
2. Select a Mercury LED Mode table.
3. Review the table details. For any door State, any of the following can be updated:
   - Change the color that displays when the state becomes:
     - Active in the **On Color** column.
     - Inactive in the **Off Color** column.

     Select the color from the list. For example:

     
     
   - Change the duration that the color displays when the state becomes:
     - Active in the **On Time (1/10s)** column.
     - Inactive in the **Off Time (1/10s)** column.

     The time is in 1/10th second ticks.
   - To edit the number of times the LED blinks (where this is possible), enter the new value in the **Repeat Count** column.
   - To edit the number of time the blinking is accompanied by a sound (where this is possible), enter the new value in the **Beep Count** column.
4. Click **Save**.

### Restoring to Default States

- Click **Restore to Default**.

# Mercury Security LED Mode Table page

Edit any of the LED Mode tables in **Physical Access** > **Mercury LED Modes**.

> **Note:** The actual output from the selections below (in terms of colors and beeps) may vary from those selected depending on panel, reader type and configuration. For more information about the colors supported, refer to the reader manufacturer documentation.

| | |
|---|---|
| **LED ID** | The unique identifier for the LED state. |
| **State** | The door state that you can set a custom LED mode for. |
| **On Color** | The color to display when the door state is active. For more information, see *Editing LED Modes* on the previous page. |
| **On Time (1/10s)** | The time in 1/10th second ticks that the On color will display for. |
| **Off Color** | The color to display when the door state is not active. For more information, see *Editing LED Modes* on the previous page. |
| **Off Time (1/10s)** | The time in 1/10th second ticks that the Off color will display for. |
| **Repeat Count** | The number of repeats for the on and off colors.<br>**Note:** This will not be editable for some states. |
| **Beep Count** | The number of beeps to sound when the related state becomes active.<br>**Note:** This will not be editable for some states. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Restore to Default** | Click to restore the selections for all states to their default setting. |

# LED Modes for Mercury Security

For Mercury Security door controllers, there are three reader LED modes. Each mode consist of two attribute sets:

- Door mode attributes (LED IDs 1 to 8)

  Used when the reader is idle. Repeat and beep counts can not be set for these LED IDs.

- Door processing attributes (LED IDs 11 to 15)

  Used when a card or pin is presented at the reader. Repeat count can be set for LED IDs 11 and 12 only. Beep counts cannot be set for any of these function IDs.

Mercury Security has 3 built-in **LED modes**. The following tables describe the settings for each mode.

**Figure 7: An example of the default settings for LED modes**

### Mercury LED Mode Table 1

| LED ID | State | On Color | On Time (1/10s) | Off Color | Off Time (1/10s) | Repeat Count | Beep Count |
|---|---|---|---|---|---|---|---|
| 1 | Disabled | red | 29 | off | 1 | 0 | 0 |
| 2 | Unlocked | green | 29 | off | 1 | 0 | 0 |
| 3 | Locked | red | 29 | off | 1 | 0 | 0 |
| 4 | Facility Code Only | red | 1 | off | 29 | 0 | 0 |
| 5 | Card Only | red | 1 | off | 29 | 0 | 0 |
| 6 | PIN Only | green | 1 | off | 29 | 0 | 0 |
| 7 | Card and PIN | red | 1 | off | 29 | 0 | 0 |
| 8 | Card or PIN | green | 1 | off | 29 | 0 | 0 |
| 11 | Denied | red | 2 | off | 2 | 5 | 3 |
| 12 | Granted | green | 2 | off | 2 | 7 | 1 |
| 13 | Prompt for user command | green | 1 | off | 14 | 0 | 2 |
| 14 | Prompt for second user | green | 1 | red | 4 | 6 | 2 |
| 15 | Prompt for second PIN | green | 4 | red | 1 | 25 | 2 |

# Configuring Card Formats

Readers that control access to doors come in many varieties and use many different card types.

## Supported Card Formats

The ACM system supports the most common card types using the following card formats:

- **ABA Mag**: for magnetic stripe cards.
- **Wiegand**: for other card types, including proximity cards and smart cards. These include most newer cards that use embedded chips and proprietary formats, which are now widely used due to increasingly stringent security requirements.
- **Large Encoded**: for internal numbers that are larger than 64 bits. For example, 128-bit and 200-bit cards need the 32-character Federal Agency Smart Credential Number (FASC-N) or Card Holder Unique Identifier (CHUID) for PIV-I cards. Large Encoded card formats are used with FIPS 201 compliant pivCLASS readers.

You can define custom card formats, which allow a panel to control access for a variety of readers. When you configure a door, you specify the card formats that are accepted at that door. A door can support up to 16 card formats from a system-wide total of 128 card formats. All of the doors on a single panel can collectively use at most 16 distinct card formats.

**Important:** A panel that is configured to accept the Large Encoded card format can not accept

ABA Mag or Wiegand formats. However, the panel can only accept up to 16 distinct Large Encoded card formats. Conversely, a panel that can accept any combination up to 16 of both ABA Mag or Wiegand formats cannot accept any Large Encoded card formats.

## Corporate Card Mode for Using Facility Codes

For Wiegand cards

Corporate card mode enables you to create batches of unique card numbers using different facility codes and the same range of internal card numbers. For example, two batches of 26-bit Wiegand cards can have facility codes 55 and 105 (respectively) and the same 1400-19999 internal card numbers. The facility code that is inserted at the start of each card number string can be used to grant access and then easily viewed in Monitor Events and Transaction Reports.

To use the Corporate card mode setting:

1. On the Card Format: Add or Card Format: Edit page, enter:

| | |
|---|---|
| **Facility Code** | The facility code of the card format.<br>Example: `55` for the 26-bit Wiegand card format |
| **Facility Code Length** | The length of the facility code in digits.<br>Example: `8` for the 26-bit Wiegand card format |
| **Facility Code Location** | The starting location of the facility code in the number string.<br>Example: `3` for the 26-bit Wiegand card format<br>Up to 2 zeroes (0) may be inserted at the 3-bit location. |
| **Offset** | The offset number for the card format. Used with **Corporate card mode**.<br>Example: `10000`<br>**Tip:** Any number can be used, however, a power of 10 higher than the card number used is recommended. For example, if the internal card number range is 1400-19999, specify `100000`. Your range of card numbers will now increase to 5501400-5519999.<br>When the **Offset** value is set to zero (`0`), the card number is always read from the card. |
| **Corporate card mode** | A checkmark to enable the combination of values entered in the **Facility Code** and **Offset** fields, and the card number read from the card, to produce unique card numbers that the readers at different facilities will recognize.<br>Example: `55` x `10000` + `1400` = 551400<br>**Note:** When **Corporate card mode** is enabled, the **Facility Code Length** and **Facility Code Location** values also need to be specified. |

   To enter other card format options, see *Card Format Fields* on page 309.

2. Click ✔.
3. Repeat the above steps for another facility code.

   Example: `105`
4. When the cardholder swipes the token that is configured with Corporate card mode, the cardholder is granted access to the door.

## Issue Level Numbering for Reusing a Card Number

For ABA Mag and Wiegand cards

An issue level enables a card number to be reused by creating the token for a card number with an updated issue level. Only one token for a given card number can be active at a time. If your ACM deployment uses the Issue Level numbering option in a custom card format, complete the following:

1. On the Card Format: Edit page, enter:

| | |
|---|---|
| **Issue Level Length** | The length of the issue level number in the card number string. Used with the Issue Location and Issue Level options.<br>Example: 3-digit number for the 56-bit card format type. |
| **Issue Location** | The starting location of the issue level number in the card number string.<br>Example: 0 for the 56-bit card format type. |

   To enter other card format options, see *Card Format Fields* on the next page.

2. On the Token: Edit page, enter:

| | |
|---|---|
| **Issue Level** | A number from 0 to 999999999, representing the issue level of the token.<br>Example: If a 3-digit length was configured on the Card Format: Edit page, you can enter 123 for the issue level of the card. |

3. Click .

   When a cardholder swipes the token that is configured with an issue level, the cardholder is granted access to the door. If an issue level that is not configured is swiped (for example, any issue level that is not 123), the following door event is generated in the log: "Valid card with an incorrect issue level."
4. If the card number needs to be reused, repeat step 2 and increment the issue level number.
5. When the cardholder swipes the token that is configured with the updated issue level, the cardholder is granted access to the door.

## Adding Card Formats

1. Select **Physical Access** > **Card Formats**.
2. Click **Add Card Format**.
3. In the Card Format Add page, enter the details for the new card format.
4. Click to save the new card format.

The new card format is displayed in the Card Formats list and can be assigned to doors in the system.

## Editing Card Formats

1. Select **Physical Access** > **Card Formats**.
2. On the Card Formats list, click the name of the card format that you want to edit.
3. On the Card Format Edit page, make the required changes.
4. Click to save the changes and download the updated card format information to all panels and door subpanels that are assigned the format.

The updated card format is available on all affected doors as soon as the updated card format information is downloaded.

## Deleting Card Formats

1. Select **Physical Access > Card Formats**.
2. Click for the card format that you want to delete.
3. When the confirmation message is displayed, click **OK** and the updated card format information is downloaded to all panels and door subpanels that are assigned the format.

The deleted card format is removed from all affected doors as soon as the updated card format information is downloaded.

## Card Format Fields

Add or edit a card format from **Physical Access > Card Formats**:

| | |
|---|---|
| **Name** | The name of the card format. |
| **Card Format Type** | The card format type.<br>• **ABA Mag**—for magnetic stripe cards<br>• **Wiegand**—for other card types, including proximity cards and smart cards.<br>• **Large Encoded**—for internal numbers that are larger than 64 bits. For example, 128-bit and 200-bit cards need the 32-character Federal Agency Smart Credential Number (FASC-N) or Card Holder Unique Identifier (CHUID) for PIV-I cards. Large Encoded card formats are used with FIPS 201 compliant pivCLASS readers.See *Appendix: pivCLASS Configuration* on page 503.<br>The option you select will determine which of the following options are displayed. |
| **ABA Mag options** | |
| **Facility Code** | The facility code of the card format. |
| **Offset** | The offset number for the card format. In ABA Mag card formats, the offset value is added to the card number read from the card and the result is used as the card number for the access request. |
| **Max Digits** | The maximum number of digits for the card format. |
| **Min Digits** | The minimum number of digits for the card format. |
| **Facility Code Length** | The length of the facility code in digits. |
| **Facility Code Location** | The starting location of the facility code in the number string. |
| **Card Number Length** | The total length of the card number on the card. |
| **Card Location** | The starting location of the card number in the number string. |
| **Issue Level Length** | The length of the issue level number in the number string. |
| **Issue Location** | The starting location of the issue level number in the card number string. |

| | |
|---|---|
| **Suppress facility check** | By default, checking the facility code allows a single card format to be used for multiple sets of cards with matching number length, but different facility codes.<br><br>A checkbox to ignore a facility check. |
| **Corporate card mode** | Not supported for ABA Mag card formats. Checking this option will have no effect. |
| **Wiegand options (Mercury and HID™/VertX panels)** | |
| **Facility Code** | The facility code of the card format. |
| **Offset** | The offset number for the card format. Used with **Corporate card mode**.<br><br>• If **Corporate card mode** is disabled (the default setting), the Offset value is added to the card number read from the card and the result is used as the card number for the access request.<br>• If **Corporate card mode** is enabled, the Facility Code value read from the card is *multiplied by the Offset* value and then added to the card number read from the card. The result is used as the card number for the access request.<br><br>**Note:** When **Corporate card mode** is enabled, the **Facility Code Length** and **Facility Code Location** values also need to be specified.<br><br>When the **Offset** value is set to zero (0), the card number is always read from the card. |
| **Number of Bits** | The maximum number of bits this card format can have. If the **Reverse card bytes** option is available for this card format type and it is enabled, the value entered here must be a multiple of 8. |
| **Even Parity Length** | The length of the number string that will have even parity. |
| **Even Parity Location** | The starting location of the number string that will have even parity. |
| **Odd Parity Length** | The length of the number string that will have odd parity. |
| **Odd Parity Location** | The starting location of the number string that will have odd parity. |
| **Facility Code Length** | The length of the facility code in digits. This value must be specified if **Corporate card mode** is enabled. |
| **Facility Code Location** | The starting location of the facility code in the number string. This value must be specified if **Corporate card mode** is enabled. |
| **Card Number Length** | The total length of the card number on this card. |
| **Card Location** | The starting location of the card number in the number string. |
| **Issue Level Length** | The length of the issue level number in the card number string. |

| | |
|---|---|
| **Issue Location** | The starting location of the issue level number in the card number string. |
| **Suppress facility check** | A checkbox to ignore a facility check and use overlapping card number sequences in card sets with matching values in the bit length and bit parity fields.<br><br>**Note:** If this mode is used with **Corporate card mode**, the reader will read the facility code from the card and use it to calculate the offset. The Facility Code Only door mode cannot be used when the **Suppress facility check** checkbox is used. |
| **Corporate card mode** | A checkmark to enable the combination of values entered in the **Facility Code** and **Offset** fields, and the card number read from the card, to produce unique card numbers that the readers at different facilities will recognize.<br><br>**Note:** When **Corporate card mode** is enabled, the **Facility Code Length** and **Facility Code Location** values also need to be specified. |
| **Additional Wiegand options (Mercury panels only)** | |
| **Step parity by 2** | A checkbox to indicate that the parity must be stepped by 2.<br><br>Can only be used with cards that are encoded with this parity scheme. |
| **Enable 37 bit parity w/4** | A checkbox to enable 37-bit parity by 4 format.<br><br>Can only be used with cards that are encoded with this parity scheme. |
| **Enable 37 bit parity w/2** | A checkbox to enable 37-bit parity by 2 format.<br><br>Can only be used with cards that are encoded with this parity scheme. |
| **Enable 75 bit transparent mode** | A checkbox to enable 75-bit transparent mode for PIV/TWIC cards. |
| **Reverse card format** | A checkbox to enable the bit-level reversal of the entire bitstream from the card when it is received from the card reader. The reversed bit stream is then compared against the card format. If it matches, then the data in the card format is used to authenticate the identity of the cardholder. |
| **Reverse card bytes** | A checkbox to enable the byte-level reversal of the entire bitstream from the card when it is received from the card reader. The reversed bit stream is then compared against the card format. If it matches, then the data in the card format is used to authenticate the identity of the cardholder. For this option to correctly function, the value in the **Number of Bits** field must be a multiple of 8. |
| **Large Encoded** | |
| **Number of Bits** | The maximum number of bits the card format can have. The default value is 0. The maximum value is 128. |
| **Card Number Length** | The maximum length (in bits) of the card format. This value must be the same as the value for Number of Bits. |

| | |
|---|---|
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

# Configuring ACM System Events

The ACM system generates events to notify you of issues that may require your attention. Events include messages and alarms issued by specific devices in the ACM system.

You cannot create events but you can customize the existing system events to monitor what you are most concerned about.

Events can be made into an alarm when they are assigned to an alarmed Event Type. For more information, see *Event Types* on page 381.

## Searching for ACM System Events

The ACM system provides many events, so it may sometimes be easier to search for the specific event that you want to customize. For example if you are looking for an event related to failures in the system, you can search for events containing the word failure.

1. Select **Name** or **Event Type** in **Search Field**.
2. Select the search operator in **Search Value** and your search criteria.
3. Optional. To refine your search, click **Add Criteria**, repeat the above steps, and select the **And** or **Or** search operator (located next to the Search button).

   To remove a single criteria row, click **Remove**. To clear all fields, click **Clear Search**.
4. Click **Search**.

The results are displayed.

## Customizing ACM System Events

You can edit ACM system events to customize them to your needs. For example, if an action needs to be taken when a specific event occurs, instructions can be added to that event. These instructions will be displayed when the event is triggered.

1. Select **Physical Access** > **Events**.
2. On the Events list, click the name of the event you want to edit.

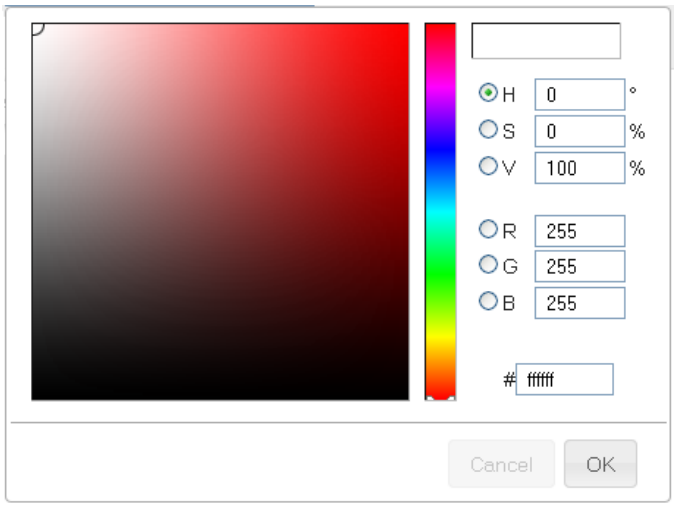
   The Event: Edit page is displayed.
3. Make the required changes.
4. Click to save your changes.

## Assigning Priority Colors to ACM System Events

You can assign a color to any priority level. The colors are used to highlight events with the same priority on the Alarms page in the Monitor screen.

The alarm priority is assigned to events on the Event Edit page or the Event Type Edit page.

1. Select **Physical Access > Events**.
2. Select the **Colors** tab.
3. On the Colors list, do one of the following:
   - To add a new color, click **Add New Color**.
   - To edit a priority color, click a listed priority number.
   - To delete a priority color, click .
4. On the following page, enter the priority number that this color set should be assigned to.
5. For each of the color options, click the color field to display the color map.



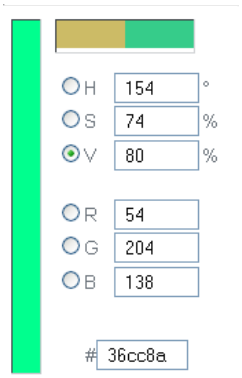

6. To use this palette to select a specific color:
   a. From the HSV or RGB color fields, enter the general color you require.

      All possible tints and variations of this color appear to the left in the tint area.

      The new color you have selected appears on the right side of the horizontal bar above the color element fields. The original color appears to the left.

   b. To fine-tune the color, click within the tint area.

      A cross appears. Drag the cross through the area to determine the exact color you want. indicating the exact tint and shade you have selected like the following example:



The number in the Color field changes to reflect your choice.

c. If required, slide up or down the vertical slide bar to change the color still further.

d. When you're finished with this palette, click **OK**.

7. Click ✔ to save.

# Global Actions

Global actions allow you to perform one or more actions simultaneously at a large number of doors connected to more than one panel. These actions can be triggered in the following ways:

- Manually, from the Global Actions list.
  From the browser or ACM Expedite mobile app.

  > **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

- By schedule, configured from the Global Actions list.
- Automatically, when used in a Global Linkage.
  One or more global actions must be defined before you can create Global Linkages.

> **Important:** A Priority Door Policy is the most secure way to control access with the ACM system in an emergency situation. It is also more robust than a Priority Door Global Action. A Priority Door Policy will stay in effect on the doors it is installed on even if:
>
> - The ACM appliance:
>  - Is restarted
>  - Is disconnected from power
>  - Fails over to a backup appliance
> - The door or door panel:
>  - Goes offline
>  - Is rebooted
>  - Is disconnected from power
>  - Is disconnected from the access control network.

# Adding Global Actions

1. Select **Physical Access** > **Global Actions**.
2. On the Global Action list, click **Add Global Action**.
3. Enter the required details for the new global action.
4. Select the objects of the global action by moving them to the **Members** list.

   To add an item, select it from the **Available** list and click ►.

   To remove an item, select it from the **Members** list and click ◄.

   > **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

5. Click ✓ to save.

After defining all your global actions, proceed to Global Linkages to create a sequence of actions.

### Adding a Group of Global Actions

Before you start, create multiple global actions.

1. Add a global action by selecting **Action Group** in the **Type** field.
2. Move the multiple global actions to the **Members** list.
3. Click ✓ to save.

# Editing Global Actions

1. Select **Physical Access** > **Global Actions**.
2. Click the name of the global action.
3. Make the required changes.
4. Click ✓ to save your changes.

# Types of Global Actions

> **Note:** Only Access Group Install/Un-Install, Action Group, Door Grant, Door Install/Un-install, Door Mask and Door Mode are applicable for ASSA ABLOY external-powered doors. Door Grant and Door Mode are not applicable for ASSA ABLOY battery-powered doors. Any locks that do not support real-time communication with a server, will not display door mode options on the Doors list page and maps. Door mode can be set on the Door: Edit page and by using a batch job (specification).

| Type | Description |
|---|---|
| **Access Group Install/Un-install** | One or more designated access groups to be installed or uninstalled. |
| **Action Group** | A group of global actions to be run. |

| | |
|---|---|
| **Area** | You can run or schedule an action in an area, like moving or clearing identities in that area. |
| **DMP Intrusion Area** | *For DMP intrusion panel only*. All available commands for intrusion areas. |
| **DMP Intrusion Output** | *For DMP intrusion panel only*. All available commands for intrusion outputs. |
| **DMP Intrusion Panel** | *For DMP intrusion panel only*. All available commands for intrusion panels. |
| **DMP Intrusion Zone** | *For DMP intrusion panel only*. All available commands for intrusion zones. |
| **Door Grant** | Entry to be granted at one or more designated doors. |
| **Door Install/Uninstall** | One or more doors to be installed or uninstalled. |
| **Door Mask** | Alarms to be forced to a mask or unmask state at one or more designated doors. |
| **Door Mode** | The door mode to be applied to one or more designated doors. |
| **Email** | The email addresses of the recipients of global action notifications |
| **Exacq Soft Trigger** | *Exacq video integration only*. A soft trigger to be run on the Exacq camera system. |
| **Input** | *Bosch intrusion panel only*. One or more designated inputs to be masked or unmasked. |
| **Intrusion Area** | *For Bosch intrusion panel only*. All available commands for intrusion areas. |
| **Intrusion Output** | *For Bosch intrusion panel only*. All available commands for intrusion outputs. |
| **Intrusion Point** | *For Bosch intrusion panel only*. All available commands for intrusion points. |
| **Output** | *For Bosch intrusion panel only*. One or more designated outputs to be activated or inactivated. |
| **Panel Install/Un-install** | One or more panels to be installed or uninstalled. |
| **Panel Macro** | *For Mercury Security panel only*. A macro command to be run on a designated group. |
| **Policy Install/Un-install** | *For Mercury Security door only*. One or more designated policies to be installed or uninstalled. |
| **Schedule Set Mode** | One or more schedules to be activated, inactivated or scanned. |

# Deleting Global Actions

1. Select **Physical Access** > **Global Actions**.
2. From the Global Actions list, click for the global action that you want to delete.
3. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.

# Creating Global Actions and Linkages for Bosch Intrusion System

Noted below are some examples of setting up intrusion linkages and actions.

## Intrusion panel alarm due to an event in the System

An ACM system event can trigger an intrusion alarm point. To set up an alarm condition that is generated at the intrusion panel notifying the monitoring center) due to an ACM system event (for example, a forced door), ensure that the intrusion panel has a point with source "output" and select an index that is unused both as a point and as an output. Follow the steps below:

1. Create global actions to activate and deactivate the output.
2. Create a global linkage to the Forced Door event, to activate the output.
3. Create a global linkage to a NORMAL Forced Door event to deactivate the output.

When the related event occurs in the ACM system, the corresponding point will be triggered at the intrusion panel, and control over the event (for example,. silencing an alarm) can be made by intrusion panels.

### Disable and enable doors from keypad

Arming an alarm at the intrusion keypad can also lock a door within the ACM system.

1. Create global actions to lock and restore the door.
2. Create a global linkage to the area arming events, to lock the door.
3. Create a global linkage to the area disarming events, to unlock the door.

It is best to set this action up with a single area as different combinations of arming and disarming could leave the door unexpectedly locked or unlocked.

Alarms and access will be accessible from the keypad and from the **Monitor** > **Bosch Intrusion Status** > **Areas** section of the ACM system.

> **Note:** Keypad access will be limited by the tokens assigned to the identity.

### Disarm Alarm on Access Grant with restricted authorities

Accessing an area by a valid the ACM system card access can automatically disarm an area.

To allow a scenario where entry to an area by a valid card access disarms an intrusion area based on the badge holder's intrusion authorities, follow the steps below:

1. Create a global action to disarm an area. Action type of 'Intrusion Area', Subtype 'Primary Disarm' and the relevant areas as the Members.
2. Create a global linkage to door access events.
    - Devices tab: Door as the Type and the target doors as Members.
    - Events tab: Local Grant.
    - Actions tab: Disarm All.

Areas can be armed and disarmed from the keypad (depending on the tokens assigned to the identity) and from the **Monitor** > **Bosch Intrusion Status** > **Areas** section of the ACM system.

## Creating Global Actions and Linkages for DMP Intrusion System

An example of setting up intrusion actions and linkages is provided below.

### Toggle Arming and Disarming Areas

1. Create a global action to run the Toggle: Arm / Disarm mode.

   For example, enter:

   - **DMP Intrusion Area** in **Type**.
   - **Refuse Arm** in **Sub-Type**.
   - A checkmark in **Toggle: Arm / Disarm**.
   - In the **Members** box in **DMP Intrusion Areas**:
     - *Area 1 on Panel A*
     - *Area 2 on Panel A*
     - *Area 3 on Panel A*
     - *Area 1 on Panel B*
     - *Area 2 on Panel B*
     - *Area 3 on Panel B*

   For more information, see *Adding Global Actions* on page 315.
2. Run each global action by clicking **Execute** on the list of global actions.
3. View the status changes on **Monitor** > **DMP Intrusion Status**:
   - An Armed area becomes Disarmed.
   - A Disarmed area becomes Armed.

   For more information, see *Monitoring and Controlling DMP Intrusion Systems* on page 56.
4. To run them on a schedule, see *Scheduling a Global Action* on page 460.

   To run them as arm or disarm events are generated, see *Global Linkages - Introduction* on the next page.

## Searching for Global Actions

View all the global actions that have been configured in the ACM system on the **Physical Access** > **Global Actions** page.

To narrow down the search results:

1. Select **Name**, **Show in ACM Expedite**, **Type**, or **Partitions** in **Search Field**.

   **Partitions** is displayed only if partitions are defined in your ACM system.
2. Select the search operator in **Search Value** and your search criteria.
3. Optional. To refine your search, click **Add Criteria**, repeat the above steps, and select the **And** or **Or** search operator (located next to the Search button).

   To remove a single criteria row, click **Remove**. To clear all fields, click **Clear Search**.
4. Click **Search**.

The results are displayed.

| | |
|---|---|
| **Name** | The name of the global action.<br>Click the name to edit the global action. |

| | |
|---|---|
| **Type** | The type of action performed by the global action. For more detail, refer to *Types of Global Actions* on page 315. |
| **Show in ACM Expedite** | Shows the global action in the ACM Expedite mobile app, if checked (default).<br>indicates the global action is not displayed in the app.<br>Click the icon to change the setting. |
| **Run** | Click **Execute** to manually initiate the global action. |
| **Schedule** | Click **Schedule** to create a batch job for the global action. For more information, see *Scheduling Batch Jobs* on page 455. |
| **Delete** | Click to delete the global action. |
| **Add Global Action** | Click the button to create a new global action. |

# Global Linkages - Introduction

Global linkages are the final step in the process that defines specific actions for triggering events at specific doors. What separates this procedure from the Macro or Trigger features available for specific doors or panels, is that this feature is capable of connecting many doors and inputs spread across many panels.

For example, you could lock down an entire building simply by issuing a single trigger. At a more sophisticated level, you can use global linkages to plot a complex scenario, like a sally port or a man trap, in which a series of doors are opened in sequence, inputs associated with those doors are sequentially masked and unmasked, and cameras are turned on as each door is opened.

Global linkages allow you to plan a cascade of triggers and their resulting actions with only a single code entry or command.

## Searching for a Global Linkage

You can search for global linkages by search criteria, such as name, schedule, or appliance.

1. Specify your **Search Field** in the drop down list.
2. Select any needed conditions from the **Search Value** drop down list.
3. To add more search criteria, do the following, otherwise proceed to step 4:
    a. Click **Add Criteria**.
    b. Repeat steps 1 to 2.
    c. Select either:
        - **And** to find all identities that fit all entered criteria.
        - **Or** to find identities that fit one or more of the entered criteria.
    d. Continue adding search criteria as needed.
4. Click **Search**.
   The page displays your search results.

To clear all fields, click **Clear Search**.

To remove a search row, click **Remove**.

## Adding Global Linkages

1. Select **Physical Access** > **Global Linkages**.
2. On the Global Linkage list, click **Add Global Linkage**.
3. Enter the required details and click .
4. Edit each tab to add the required events, devices, identities and actions.
5. Click to save your changes on each page.

## Editing Global Linkages

1. Select **Physical Access** > **Global Linkages**.
2. On the Global Linkage list, click the name of the global linkage that you want to edit.
3. Edit each tab as required.
4. Click after editing each page to save your changes.

# Mustering

In emergency situations, employees and other personnel in your building may be required to gather at specific locations so emergency response teams can work quickly to ensure that everyone is safe. For example in a fire drill you may be asked to wait at a specific spot, or muster station, until the drill is over. This would be the same spot you would gather in an actual fire.

To help track the location of users in emergency situations, Access Control Manager offers the Mustering feature. Mustering allows you to create a dashboard to quickly monitor who has arrived at their muster station and who is still in danger during emergency situations.

## Mustering - Requirements

To use the Mustering feature, you must configure each muster station and give users access to it in the ACM system.

1. Create an area for each muster station. For more information, see *Adding Areas* on page 301.
2. To organize related areas together, you can combine them into groups.
3. Identify all the doors that lead to the muster station area, then make sure the correct area is assigned to each door.
   a. In the Access Control Manager software, select **Physical Access** > **Doors**.
   b. Click the name of the door that should be in the area, then select the Operations tab.
   c. From the **Into Area** drop down list, select the area the door enters into.
   d. From the **Out of area** drop down list, select the area the door exits from.
   e. Click .
4. Create an access group that includes all the doors in the muster station area.

5. Assign the access group to a role that would need access to the mustering area.

> **Tip:** Create a role for each mustering area. If users physically move locations within an organization, they can be easily assigned to new mustering stations without impacting their primary role in the system.

6. Assign the role to each identity that would need access to the muster station.

Next, create a dashboard to track identities as they arrive at the appropriate muster station in emergency situations.

## Mustering - Creating a Dashboard

A Mustering dashboard is a map that contains a quick view of who has entered each muster station area.

The dashboard can be a simple list of all the Mustering areas, or it can be configured into color coded shapes for quick identification.

You can add a dashboard to any map, or you can create a blank map to host the dashboard.

1. Select > **Maps**.

   The Map Templates list is displayed.
2. In the Map Templates list, decide if you want to add a dashboard to an existing map or create a blank map.
   - To add the dashboard to an existing map, click the name of the map you want to use.
   - To create a blank map, click **Add New Map Template** then check the **Use Blank Canvas** box.

     Complete the other details and click .
3. On the Map Template Edit page, click **Add** beside Dashboard Elements.
4. Enter a title for the dashboard element. The map automatically updates with each change that you make.
5. Click the **Title Font Color** field to change the text color.
6. In the **Title Font Size** drop down list, select the size. The options are Small, Medium and Large.
7. For the **Opacity** option, choose how transparent you want the dashboard element to be. You can enter a percent number, or move the slider to set the opacity. 100% is opaque and 0% is transparent.
8. In the **Location** field, enter where you want the dashboard element to appear on the map. You can also move the dashboard element directly on the map.
9. In the **Element Type** drop down list, select if you want the dashboard element to appear as Text Only or Graphic & Text.

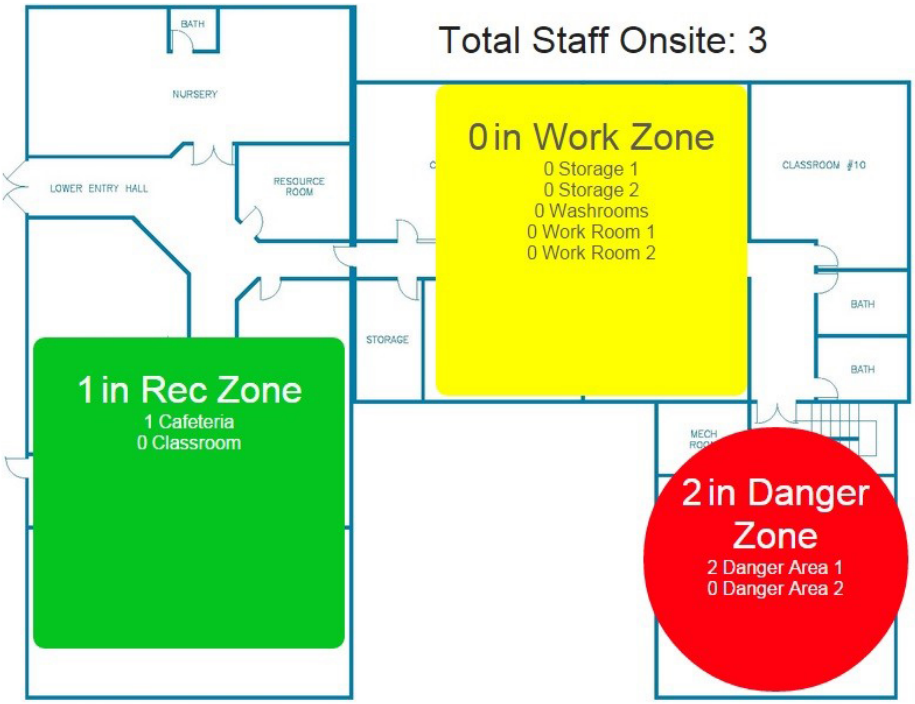
   If you choose Graphic & Text, the following options are displayed:
   a. In the **Area Group/Area** drop down list, select the muster area this dashboard element represents. You can select a specific area or a group of areas.
   b. From the **Graphic Shape** drop down list, select Circle or Square.
   c. Click the **Graphic Color** field to change the graphic shape color.
   d. For the **Graphic Size** option, choose how big you want the graphic to be. You can enter the size in pixels, or use the slider to adjust the size.
10. Click to save your changes.

To use the dashboard, see *Using a Map* on page 432.

# Mustering - Using the Dashboard

Once you have the Mustering dashboard set up, you can monitor access to each muster station area in the event of an emergency.

1. Select **Monitor** > **Maps**.
2. Select the Mustering dashboard from the Map  list.




**Note:** Depending on how your dashboard is set up, your map may look different. Dashboard elements may appear as a line of text or as a shape with text inside.

Each dashboard element is labeled in this format: *<# people> <Area Name>*. The title of each dashboard element displays the total number of people that are in the grouped area, and listed below the title is a list of each area within the group.

As people move from one area to the next, you can track who is still in the danger area and who has arrived in a safe area.

3. Click a dashboard element to display a list of all the people who are in an area.

Click the name of a person on the list to go to their Identity page. The Identity Edit page will tell you the last door and area this person accessed.

4. To generate a report of all the people in each area, select **Reports** > **Area Identity Report**.

   By default, the report displays a list of identities that are in each configured area, but you can filter the list to display only specific areas.

## Updating or Clearing the Area of an Identity

In an emergency situation, it is hard to anticipate how people will move and arrive at their mustering stations. If someone chooses to follow another to their mustering station and does not check-in with their badge, you can manually set the identity as having arrived to a safe Mustering area.

> **Note:** Confirm the location of the person before you reset their actual location in the system.

1. Select **Identities**. Click the name of an identity.

   In the Identity Information area, the last door and area accessed by the person is displayed.
2. Select the **Tokens** tab.
3. In the **Last Area** drop down list, select the specific area that the person is currently located.
   If the person has left the location entirely, such as going home, you can leave the **Last Area** blank.
4. Click .

To move multiple identities in an area to a new area, see *Moving Identities between Areas* below.

To clear multiple identities in an area, see *Clear Identities from an Area* on the next page.

## Moving Identities between Areas

Instead of manually moving the identities one at a time, you can also move identities in bulk from one area to another.

> **Note:** Confirm the location of the person before you reset their actual location in the system.

1. Select **Monitor** > **Dashboard**.
2. Select **Areas**. A list of the defined areas is displayed.

   You can also move identities between areas on **Maps**.
3. To move all identities to another area:
   a. Select each area with the identities you want to move.
   b. Click **Move Identities** , select the new area, and click **Move to**.
      All identities in the selected areas move to the area you specified.
4. To move some, but not all, identities to another area:
   a. For the area you want to move identities from, select the link in the **Number of Identities** column to open the area identities screen.
   b. Select the identities you want to move and click **Move Identities** .
   c. Select the new area, and click **Move to**.
      The selected identities move to the area you specified.

You can also move identities by altering the **Last Area** value, see *Updating or Clearing the Area of an Identity* on the previous page.

## Clear Identities from an Area

> **Note:** Confirm the area is empty before you clear it in the system.

1. Select **Monitor** > **Dashboard**.
2. Select **Areas**. A list of the defined areas is displayed.
   You can also move identities between areas on **Maps**.
3. To clear all identities:
   a. Select the areas with the identities you want to clear.
   b. Click **Clear Identities**.
   All identities are removed from the areas you selected.
4. To clear some, but not all, identities:
   a. For the area you want to clear identities from, select the link in the **Number of Identities** column to open a pop-up.
   b. Select the identities you want to remove and click **Clear Identities**.
   The selected identities are removed from the area you specified.

## Using Global Actions to Move or Clear Areas

You can use global actions to schedule area actions, like moving or clearing identities.

1. Select **Physical Access** > **Global Actions**.
2. On the Global Action list, click **Add Global Action**.
3. Name the action.
4. Select **Area** in the Type field.
5. To move identities:
   a. Select **Move Identities** in the Sub-Type field.
   b. Select the **Target Area**.
   This is the area where you want to move the identities.
   c. Select one or more of the **Available** areas and move it to the **Members** list.
   This is where the identities originally reside, before moving them to the **Target Area**.

   To add an item, select it from the **Available** list and click ►.

   To remove an item, select it from the **Members** list and click ◄.

   > **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

   d. Click ✔ to save.

6. To clear identities:
   a. Select **Clear Identities** in the Sub-Type field.
   b. Select one or more of the **Available** areas and move it to the **Members** list. These are the areas you want to clear of identities.

      To add an item, select it from the **Available** list and click ►.

      To remove an item, select it from the **Members** list and click ◄.

      > **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

   c. Click ✔ to save.

For details, see *Adding Global Actions* on page 315.

# Managing Appliances

When you log in to the ACM application, you are accessing an appliance that is set up in your network. The appliance configures and directs communication between all the elements in the access control system.

After you have connected your appliance to the network, you can further customize and set up your appliance to meet your system requirements.

## Editing Appliance Settings

After initial setup, you can edit the ACM system settings and set up backup and redundancy for the appliance.

1. In the top-right, select > **Appliance**.

   If only one appliance is managed by the system, the Appliance Edit page is displayed.

   If more than one appliance is managed by the system, the Appliance list is displayed. Select the appliance you want to edit.
2. Navigate through the following tabs to configure the appliance:
   - **Appliance** tab: Edit system, network and storage settings, as well as shut down or restart the appliance remotely.
   - **Access** tab: Specify and enable the controller panel types.
   - **Ports** tab: Specify how the Ethernet ports on the appliance are used to communicate with access control devices, including DHCP.
   - **Replication** tab: Set up system replication and redundancy.
   - **Backups** tab: Set up scheduled backups for the appliance.
   - **Logs** tab: Access the system logs.
   - **Software Updates** tab: Update the appliance software.
   - **SSL Certificate** tab: Configure SSL certificates used in the authentication of ACM Client users. For more information, see *Configuring Remote Authentication Using SSL Certificates* on page 391.
   - **About** tab: View and manage licenses, and view the version numbers and End User License Terms and Conditions.
3. Click to save your changes.

## Deleting an Appliance

Appliances may need to be deleted in certain cases. If you want to disconnect an appliance that is no longer needed, delete it from the system before physically removing it. If you want to take an appliance that is being used for replication or redundancy and use it as a primary appliance, the appliance must be deleted first.

**Note:** You can only delete an appliance if your system has more than one appliance.

1. In the top-right, select > **Appliance**.
2. From the Appliance list, click beside the appliance that you want to delete.
3. When the confirmation message is displayed, click **OK**.

The selected appliance is removed from the list.

# Configuring Replication and Failover

The Replication tab on the **Appliance: Edit** page allows configuration and monitoring of LDAP data replication and optionally redundancy/failover of the ACM application so that monitoring and hardware control is not lost even if an appliance fails. Only the default Admin identity can edit the appliance Replication settings.

> **Important:** The ACM 6 license format is different from previous versions. You will need to upgrade your license format if you upgraded from ACM 5.12.2 to ACM 6.0.0 or later in order to add new licenses. Replication features, including failover, will not function if your license format is not the same on both the primary and standby appliances.

The replication feature allows two or more appliances to be set up to share a single set of LDAP configuration data, so that the appliances can share identities and other system details. Any change made to configuration data on one appliance is automatically copied ("replicated") to the other appliances. This is referred to as a "Peer to Peer" configuration. In this configuration, each appliance "owns" the hardware installed on it, and events and status information sent from that hardware can only be viewed on the hardware owner appliance. All panel hardware added in a replicated environment must be assigned upon creation to one of the available Peer to Peer appliances. A panel and its subpanels cannot be split across multiple appliances, but is installed on one of the Peer appliances.

> **Tip:** It is recommended that replication be set up on all appliances before adding panels, other hardware or user details to the system. After replication is configured, it is possible to configure system hardware and identity information from one of the replicated appliances on the network rather than having to connect directly to each individual appliance to make changes to its installed hardware. However, it may be necessary to perform a download of the hardware configuration from the appliance where the hardware is installed in order to update the hardware with the latest configuration data changes made from another appliance.

## Failover/Redundancy Feature

The failover, or redundancy, feature of replication allows a "Hot Standby" appliance to be set up to take over control and event monitoring when the Primary appliance used in daily operations fails. This configuration is referred to as Primary/Hot Standby. To use the failover feature, both appliances are originally configured with Peer to Peer replication so that each appliance will share a common LDAP configuration database. The Hot Standby appliance is then configured as such, and then will not have its own hardware or collaborations, and will not appear in the list of replicated appliances available for assignment when these items are created.

Each Primary appliance can only be assigned one Standby appliance, but the same Standby appliance can

be assigned to more than one Primary appliance. However, if two or more Primary appliances fail at the same time, the Standby appliance will replace the first appliance that it knows is offline (if configured for automatic failover), and will not be available for failover of the other Primary appliances while it is standing in.

The following types of failover and failback are supported:

- Automatic failover
- Manual failover
- Manual failback

### Automatic failover

Automatic failover is controlled by the Standby appliance by monitoring the health of the Primary appliance. If a Primary appliance is found to be unresponsive by the Standby appliance within a set period of time, the Standby appliance will automatically initiate failover of the Primary appliance and will begin to control the hardware installed on that Primary appliance, and will begin to receive events and status from this hardware.

There are two settings that control automatic failover - Heartbeat count and Heartbeat time. The Heartbeat count is the number of health checks the inactive hot standby appliance makes to see if the active primary appliance is alive. If this number of failures occurs in a row, the hot standby will do an automatic failover. The Heartbeat time is the time between health checks (regardless of if the previous check was successful or failed).

It is not necessarily possible to calculate specifically how long it would take to failover. It is not simply a matter of multiplying the Heartbeat count by the Heartbeat time (for example Heartbeat count of two and Heartbeat time of 30 seconds does not necessarily mean failover in about one minute of the primary going down, however one minute would be the best/shortest case). This is because the time it takes each check to fail may depend on a network time-out in the case of the hot stand by machine no longer having network connectivity to the primary machine. Typically, a worst case network time-out is approximately two minutes - however this may possibly vary. A health check may also fail immediately depending on network considerations/status.

It is recommended to set the Heartbeat count to at least a value of two so that a short network glitch does not cause a premature failover. A Heartbeat count of two and a Heartbeat time of 30 seconds should typically ensure that a failover is initiated within one to about five minutes of the primary going down.

### Manual failover and failback

A manual failover can be initiated through from the Replication tab on the **Appliance: Edit** page on the Standby appliance. This is usually done to test functionality or if a Primary appliance is going to be down for scheduled maintenance.

Once the Primary appliance is back online and fully functional, you can then manually initiate failback of the Standby appliance over to the Primary appliance, which restores hardware control and event and status reporting to the Primary appliance.

Read through all of the following procedures before configuring replication and redundancy. If any detail is unclear, contact Avigilon Technical Support for more information before you begin.

## Recommended System Architecture

### System Architecture for Replication

Replication works by automatically copying the **LDAP**[1] configuration databases from one appliance to

---

[1]Lightweight Directory Access Protocol is an open, industry standard application protocol for accessing and maintaining distributed directory information services over a network. An LDAP database in the Access Control Manager system typically includes user details, connected hardware details, events, alarms and other system configuration details.

another. Changes made in one appliance's database are automatically replicated to the all of the other appliances. Replication can occur between two or more Peer to Peer appliances, or it can occur between a Primary appliance and its Standby appliance, and a mix of both configurations is possible.

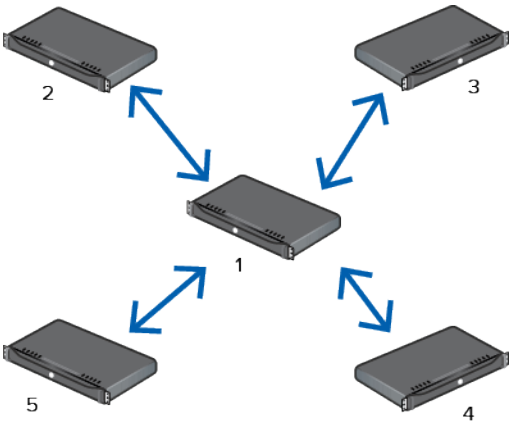
If you only have one appliance in your system, replication is not possible. In this situation, performing periodic backups is the recommended method of ensuring appliance recovery after a failure.

When two appliances exist, they can start replicating information.

Once replication is set up, any identity or other system configuration data that is added to or edited on one appliance is automatically copied to the other appliances. Be aware that each appliance will be responsible for their connected panels, subpanels, and other hardware. Configuration and viewing of all system hardware is possible from any replicated Peer appliance, but you will not be able to see the hardware status or events from any appliance other than the one the hardware is installed on.

When more than two replicated Peer appliances exist, it is recommended that Peer to Peer replication be set up in a mesh formation, where every Peer appliance has links ("subscriptions") to all of the other Peer appliances. This allows system configuration to be performed from one Peer appliance and have the details automatically replicated to all the other Peer appliances, while providing multiple paths for this data to replicate among the participating appliances. The exception to this is a Standby appliance, which only needs to have replication subscriptions with its Primary appliance.

> **Note:** Up to 99 appliances can be connected together for Peer-to-Peer replication, and this limit includes any Hot Standby appliances in the environment.




## System Architecture for Redundancy

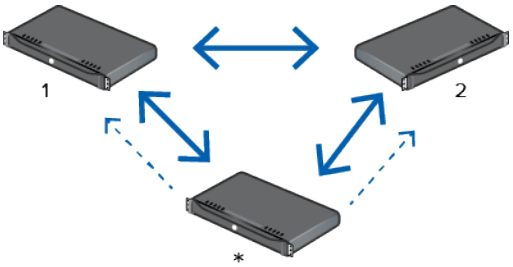
Redundancy works by having a configured Hot Standby appliance automatically or manually replace a failed Primary appliance. Redundancy requires Peer to Peer replication between the Primary and the Standby appliances to be configured and tested first to function properly. Once this is in place, the Standby appliance is then designated as such and the software configures it for that role.

When configured and in standby mode, the Standby appliance is essentially a blank appliance that only has basic system settings. The Standby appliance has its own configuration for appliance related attributes such

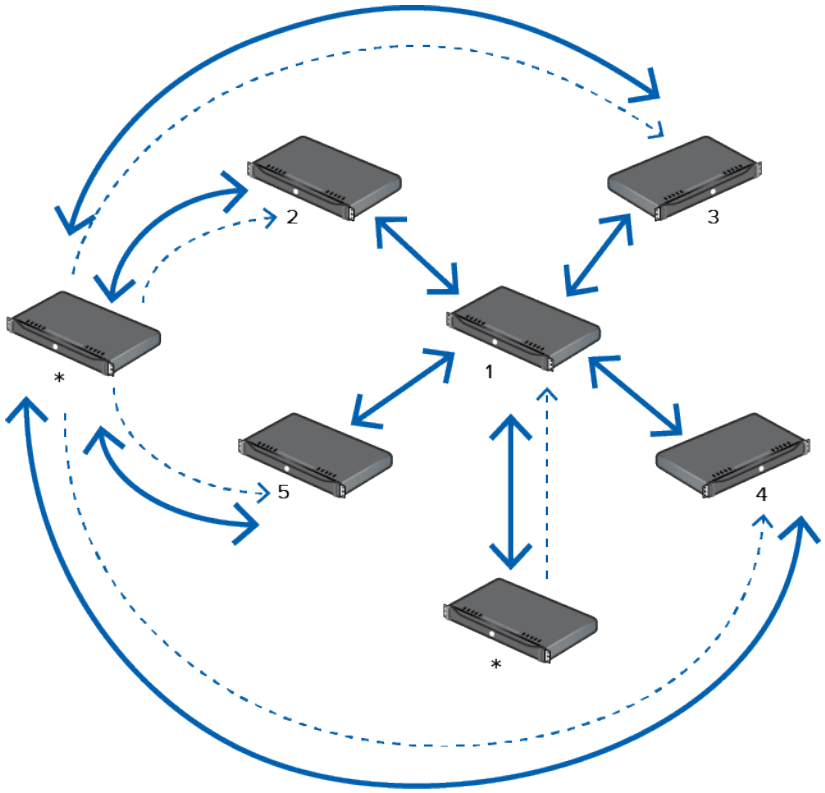
as host name, ports, time zone (etc.), but it does not have any hardware configuration of its own. It only has that hardware data which is replicated from the Primary appliance that owns it. When a Standby appliances takes over for a Primary appliance, the operating system settings on the Standby appliance (such as host name and IP address) do not change to match the Primary appliance's settings. Instead, the applications running on the Standby appliance begin to service the records (including doors, panels, video servers, collaborations and so on) previously controlled by the Primary appliance. Note that this requires a different URL for clients to be able to access the Hot Standby appliance – this is not handled automatically by the ACM system.

If one Primary appliance (1) exists for everyday operations and one Hot Standby appliance (*) is available, set up the Standby appliance to subscribe to and receive replicated configuration data and transactional data from the Primary appliance. If the Primary appliance fails, the Standby can automatically step-in and maintain daily operations.

If more than one Primary appliance exists for a Hot Standby appliance, the Hot Standby appliance still remains separate from daily operations but must receive replicated configuration and transaction data from all Primary appliances it is configured to failover for. Be aware that the Standby appliance can only stand-in for one failed Primary appliance at a time.




If the replicated environment with multiple appliances is configured in a mesh formation for replication where possible, but due to some physical limitation such as a Wide Area Network (WAN) being involved one or more of the appliances is a single point of failure for propagation of replicated data, it is recommended that each of these appliances have its own Hot Standby appliance. In the event of a failure of one of these critical Primary appliances, the environment is guaranteed to have a Hot Standby appliance available to ensure that all replicated Peer appliances are able to continue to synchronize configuration data amongst themselves.




## Replication and Failover Requirements

**WARNING —** Make sure your system meets all the following requirements before you set up replication and failover or the system may lose configured system data.

- License requirements:
  - The application license agreement must be entered on all appliances. The license key is tied to a specific machine. When using redundancy, a license and key must be separately installed on both the Primary and Standby appliances. The license features on a Standby appliance needs to include all the features used by the Primary appliances it may replace.
- Network infrastructure:
  - DNS registered host names for each appliance in the enterprise. Each appliance must be able to connect to the other appliance by host name. There must be static or reserved IP addresses, proper netmask, and network gateway for each appliance.
  - Name server IP address for host name resolution. All appliances must be able to resolve all of the other appliances by host name.
  - Time Server IP address or host name. All appliances must be synchronized for time and date. This is crucial for proper replication processing. Each must utilize a time server for this purpose. The Open LDAP multi-primary replication used by the ACM software synchronizes a LDAP directory tree across multiple appliances. Each appliance supports read/write operations across an enterprise system. Conflicts are handled using a timestamp to determine the most recent record. All appliances must use a common clock base to synchronize their clocks to ensure the conflict resolution works correctly.

> **Note:** Time is based on UTC (Coordinated Universal Time) to ensure consistency across the ACM system. UTC time is transferred from the client to the server when the date/time is set.

- Defined and open TCP ports:
  - Web Server Port / Replication Subscriptions Web Port (default 443). Certain replication options require each appliance to contact each other through the web service port.

    > **Note:** The default port must be used for Allegion Schlage locks.

  - LDAP Connect Port / Replication Subscription LDAP Port (should be a unique, open TCP port that nothing else uses). This is a TCP port used for Open LDAP replication between appliances.
  - Event Replication Port (default 6052). Once a Primary/Standby appliance relationship is established, the Primary appliance will automatically transfer event transactions to the Standby appliance so event data will be available when a failover occurs. Connectivity is required for both Primary and Standby appliances using the Event Replication Port (this is a TCP port used for open SSL socket communication).
  - Replication Failover Port for heartbeat (default is NONE but should be a unique, open TCP port that nothing else uses). This is a TCP port (used for open SSL socket communication) defined on the Primary appliance only. The Standby appliance uses it to communicate with the Primary to check its health status in order to determine if an automatic failover is required, if monitoring is enabled on the Standby appliance.
  - These ports must be open across the network between the two appliances.
- Appliance replication address. A unique numeric address number must be reserved and configured for each appliance, starting at 1 and extending to 99 (confirm max count). These addresses need not be in sequence.

  > **Note:** You can have up to 99 appliances connected together for replication, including any Standby appliances configured for failover.

- Software updates. When software updates are installed, they should be installed on all appliances in a timely manner (i.e. one after the other). Note that the appliance with address 1 should always be the first appliance in the environment to have software upgrades applied to it, as any LDAP schema and data changes (adding deleting system records, massaging of data) involved are performed there and replicated out to the other appliances. The other non-address 1 appliances will not have these LDAP schema changes applied by the upgrade, so it is essential to upgrade the address 1 appliance first. The remaining appliances can be upgraded in any order once the address 1 appliance is back online after its upgrade completes.
- Recommended SMTP settings. The SMTP settings configure which mail server should be contacted to send out email and which account should be used. This is configured separately per appliance. When the Primary and Standby appliances are physically separated, sometimes by considerable distances, it is recommended to assign local mail servers for each. A mail server must be set up on both Primary and Standby appliances if you want to send email notifications for failover and failback occurrences.

## 1. Preparing Appliances for Replication and Failover

Before you can set up replication and failover, you must set up the appliances to use the required network

infrastructure and assigned ports. For more information, see *Replication and Failover Requirements* on page 331.

## Setting Up the Primary Appliance

Whether you are configuring two or more appliances to replicate to each other in a Peer to Peer system, or configuring a Primary/Hot Standby redundant failover system, designate one appliance as the replication address 1 appliance. This appliance should not be used as a Standby appliance, and will be the first appliance to have software updates applied to it.

1. Log in to the appliance that will use replication address 1.
2. On the Appliance Edit page, enter values for the following fields in the Appliance tab:
   - **Name** – An appropriate name for the appliance so that you can identify it on sight.
   - **Host Name** – The appliance's hostname on the network.
   - **Name Server** – The IP address of the DNS server.
   - **Time Server** – The name or IP address of a time server that is accessible on the network. The time on all connected appliances must be in sync. This setting is crucial for a replicated appliance.

     > **Note:** Time is based on UTC (Coordinated Universal Time) to ensure consistency across the ACM system. UTC time is transferred from the client to the server when date/time is set.

   - **Web Server Port** – The port number for accessing the appliance web service.
   - **LDAP Connect Port** – The port number for accessing the LDAP database on the appliance. This port will be used by replication to update LDAP data and will be used when other appliances are added to the replicated environment.
3. Click to save your changes.

The appliance will automatically restart if changes are made to the above fields and saved.

## Setting Up Additional Appliances

Complete this procedure for all the other appliances in your system. Besides the name and hostname, it is recommended that if possible all other settings be the same as the primary appliance, as that will avoid confusion on what ports are used and what network resources are used for time setting and name resolution.

1. Log in to the appliance
2. On the Appliance Edit page, enter values for the following fields in the Appliance tab:
   - **Appliance Name** – An appropriate name for the appliance so that you can identify it on sight.
   - **Host Name** – The appliance's hostname on the network.
   - **Name Server** – The IP address of the DNS server.
   - **Time Server** – The name or IP address of a time server that is accessible on the network. Use the same value as the replication address 1 appliance if possible.

     > **Note:** Time is based on UTC (Coordinated Universal Time) to ensure consistency across ACM. UTC time is transferred from the client to the server when date/time is set.

- **Web Server Port** – The port number used for accessing the appliance web service.
- **LDAP Connect Port** – The port number used for accessing the LDAP database on the appliance. Use the same value as the replication address 1 appliance if possible.

3. If this is a Standby appliance, select the **Hot Standby** checkbox. Also, ensure that the Max Stored Transactions setting is at least as large as the sum of this setting for all Primary appliances that the Hot Standby will be backing up.

   **Note:** Do not select this checkbox if the appliance will not be used as a Standby.

4. Click to save your changes.

   The appliance will automatically restart if changes are made to the above fields and saved.

## 2. Setting Up Replication Between Appliances

Before the appliances can automatically replicate data between themselves, you must set up each appliance to accept replication.

### Enabling Replication on the Primary Appliance

1. Log in to the appliance that is to be assigned a Replication Address of 1.
2. In the top-right, select > **Appliance**.
3. In the Replication tab, enter the following settings:
   a. **Enable Replication**: select this checkbox.
   b. **Enable Encryption** it is recommended that you select this checkbox to allow the open LDAP servers to use OpenSSL TLS encryption when replication data is transferred between appliances.
   c. **Address**: enter 1 for this appliance. If multiple appliances exist in the system, each must have a unique two digit number replication address, with this appliance being set to "1".
   d. **Identity Password**: enter a password for securing LDAP data replication. This password should be the same across all the appliances in the replicated environment.
   e. **Event Replication Port**: enter a port number that will be used by this appliance to replicate data to the other appliances. Default is 6052.
   f. **Other Fields in Replication Settings section**: leave Initial Retry Time, Initial Retry Count, Last Retry Time, Last Retry Count, Timeout, Network Timeout, and Keep Alive at their default values. These will only need to be adjusted in consultation with Avigilon Technical Support to resolve replication problems.
4. Click to save your changes.

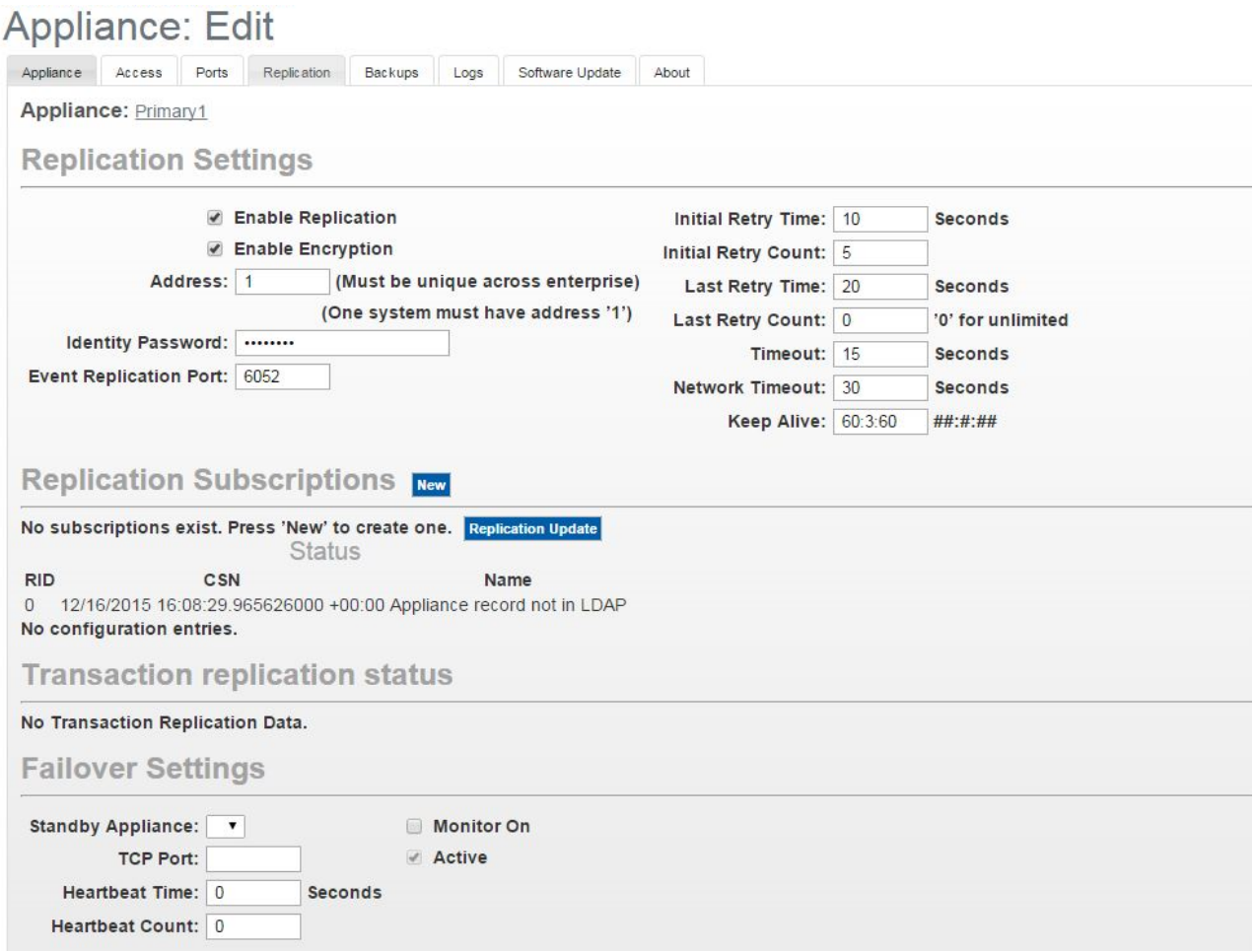



**Figure 8:** Primary Replication tab

## Enabling Replication on the Second Peer or Standby Appliance

Perform this procedure for all other appliances in the system.

1. Log in to the appliance.
2. In the top-right, select > **Appliance**.
3. In the Replication tab, enter the following settings:
   a. **Enable Replication**: select this checkbox.
   b. **Enable Encryption**: it is recommended that you select this checkbox to allow the open LDAP servers to use open SSL TLS encryption when replication data between appliances.
   c. **Address**: if you have only one secondary/standby appliance, enter 2 for the appliance. If you have multiple appliances in your system, you must enter a number from 2 to 99. You cannot use the same address twice for different appliances.

> **Note:** Up to 99 appliances can be connected together for replication, including the primary appliance and standby appliances.

d. **Identity Password**: enter the same password as used in the primary appliance.

e. **Event Replication Port**: enter a port number that will be used to replicate data to the primary appliance. Default is 6052.

f. **Other Fields in Replication Settings section**: leave Initial Retry Time, Initial Retry Count, Last Retry Time, Last Retry Count, Timeout, Network Timeout, and Keep Alive at their default values. These will only need to be adjusted in consultation with Avigilon Technical Support to resolve replication problems.

4. Click to save your changes.

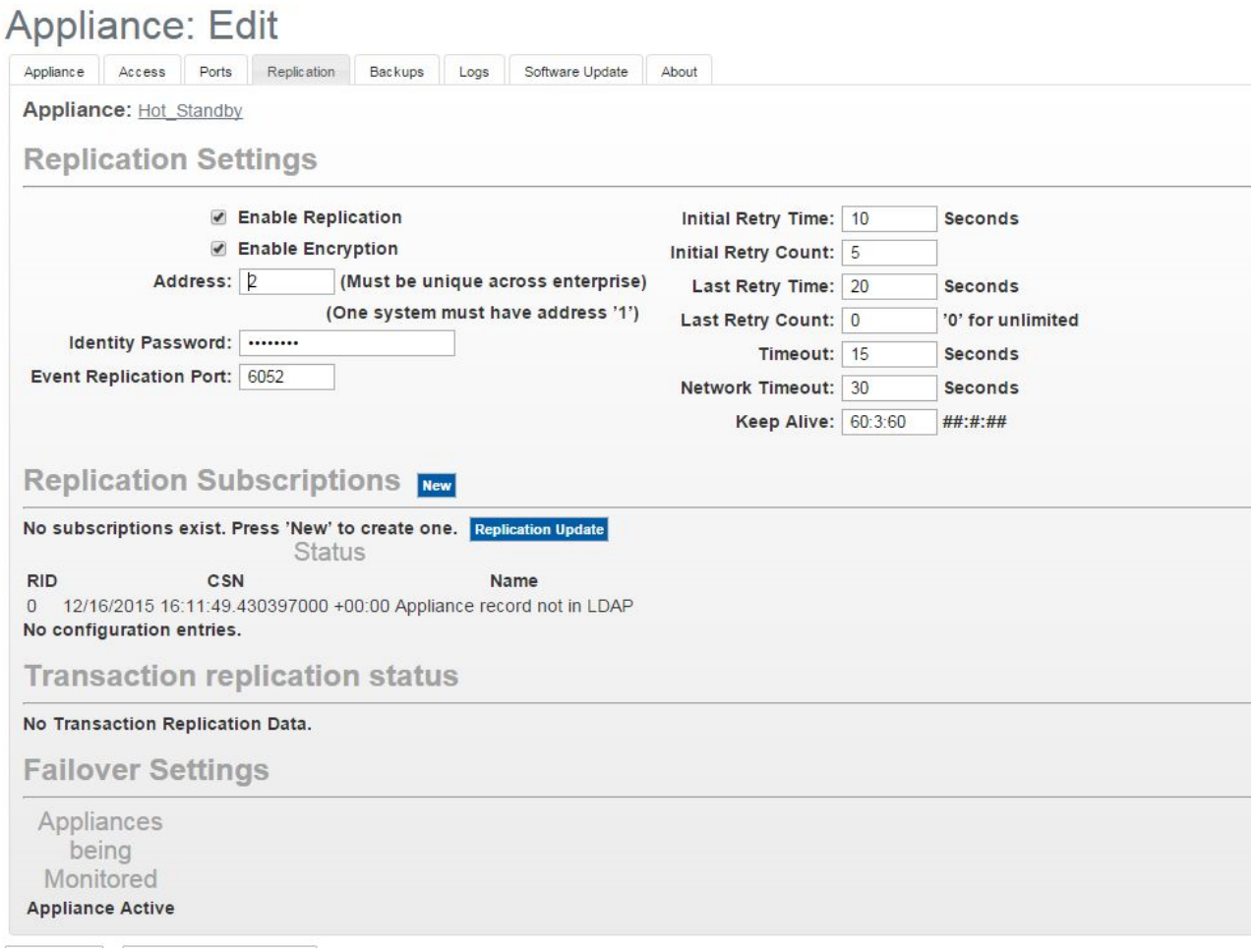



**Figure 9:** Hot Standby Replication tab

## 3. Adding a Replication Subscription

Before adding a replication subscription between the two appliances, double-check to make sure the network requirements have been met:

- The appliances are on the same network and are able to communicate with each other. Make sure the appliances are able to ping each other by host name.
- Each appliance has a time server and a name server configured for them.
- A Web Server Port, LDAP Connect Port, and Event Replication Port are configured for the appliances. Make sure these ports are open between the appliances.

- Replication has been enabled on both appliances. Both appliances have a replication identity password configured for them.
- The clocks on both appliances are in sync. The current running time can be seen on the appliance page for each appliance.

Always add the replication subscription to the first (replication address 1) appliance while logged into the second appliance and from the Hot Standby's Replication tab. As the second and subsequent appliances first subscribe to and receive replicated data from the first (replication address 1) appliance, the existing LDAP database on each subscribing appliance is overwritten by the replicated data from the first (replication address 1) appliance, so that each subscriber appliance has its LDAP data properly initialized.

Note that this overwrite of the subscriber LDAP database only occurs when the first subscription is added on a subscribing appliance. Subsequent subscriptions created on this subscriber appliance do not perform the overwrite of LDAP data that the first subscription, as the database is already initialized. This is why it is recommended that replication (and redundancy if used) is set up for each subscriber before adding hardware, user identities or system configurations to avoid data being overwritten and lost.

Do **not** add the first replication subscription to the address 1 appliance, or all configured data on that appliance will be overwritten as part of the initialization process described above.

1. Log in to the secondary or standby appliance. You must use the "admin" user name and password or you will not be able to make changes to the Replication tab.
2. In the top-right, select > **Appliance**.
3. In the Replication tab, click **New** in the Replication Subscriptions area.
4. Complete the following fields:
    a. **Host** – enter the replication address 1 appliance's host name.
    b. **Web Port** – enter the replication address 1 appliance's web port number.
    c. **Ldap Port** – enter the replication address 1 appliance LDAP Connect Port value. This is highly recommended to be the same as the LDAP Connect Port number on the current appliance.
    d. **Login** – enter an account with the proper delegations for the default administrator identity. This can be the admin account, or a different identity, can be used, but it must be an identity with the proper delegations available in its role. Delegation required for this login are Appliance Repl Subscription Add (remote), Appliance Repl Subscription Remove (remote), Appliance Replication Update and Appliances Show.
    e. **Password** – enter the password for the Login identity.
5. Click to save your changes.

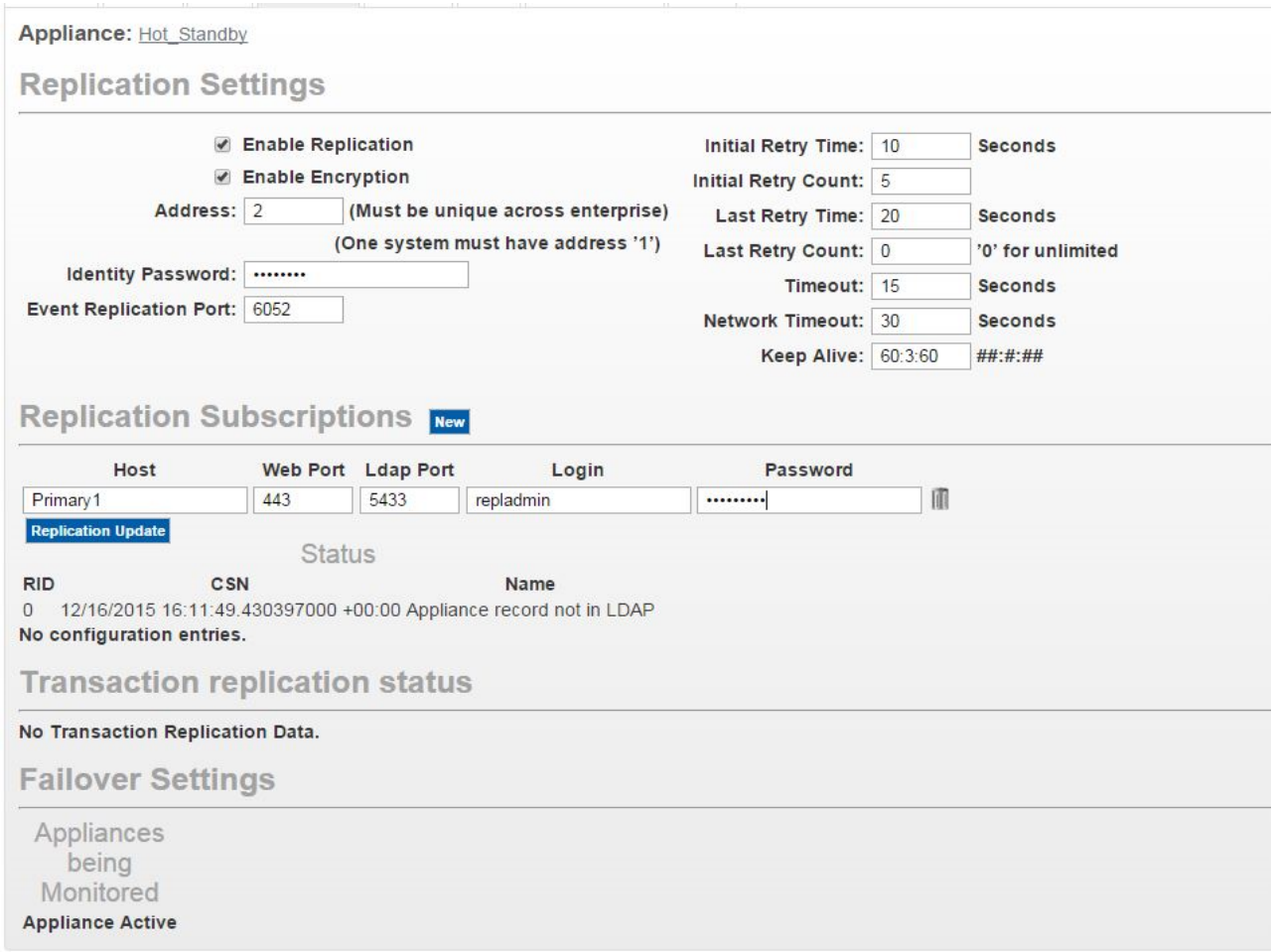



**Figure 10:** Second appliance subscribing to first appliance

The Replication Setup Process Log is automatically displayed if this is the first replication subscription. Click the Continue button that is displayed.

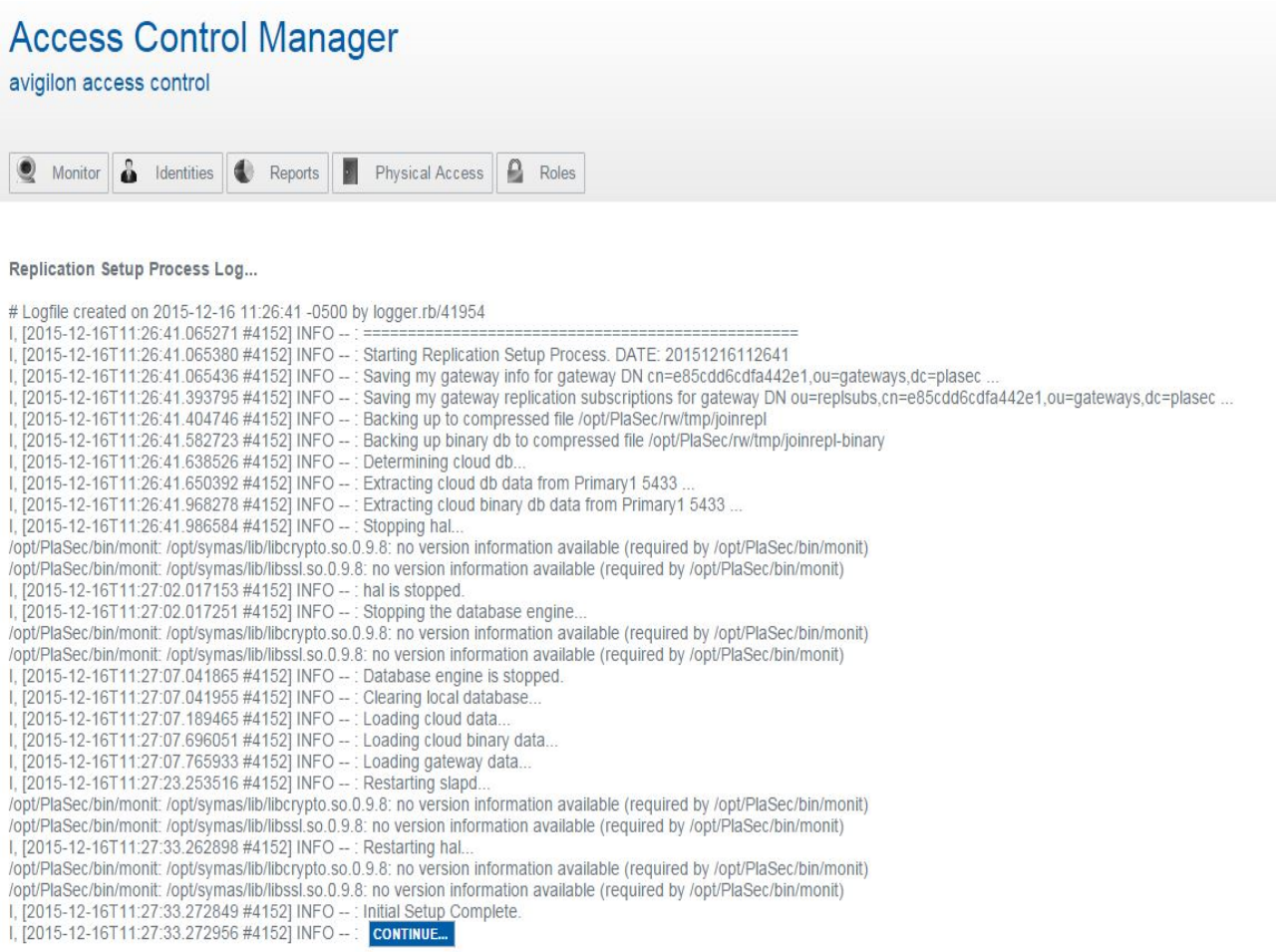



**Figure 11:** Log file on subscribing appliance

The replication set up process includes the following:

- The subscribing appliance connects to the primary appliance and copies the entire LDAP database from the primary.
- The replication subscription from the subscribing appliance to the primary is added to the LDAP configuration database.
- A replication subscription from the primary to the subscribing appliance is automatically created and added to the LDAP configuration database.

Now, complete the following tests to confirm that replication is functioning correctly.

## Testing Replication

After setting up replication between a two or more appliances, complete the following procedures to confirm that replication was set up correctly.

### *Checking the Appliance Replication Status*

Once the Replication Subscription is complete, open a browser for each appliance that is set to replicate to each other.

After you have the browsers open, display the Appliance Replication page for the appliances. Confirm that

the following settings are the same for all appliances:

> **Note:** The Status and System Entries area are only displayed if the primary and subscribing appliance details are accessed together.

- Under the Status area, 1 and 2 are listed in the RID column. 1 should be the primary appliance and 2 should be the secondary or standby appliance. There may be other numbers listed if you have more appliance subscriptions.
- Confirm that the date and time listed in the CSN column is the same for all appliances.
- Under the System Entries area, there should be at least one entry to show that the primary appliance has replicated data to the other appliances.
- When you click > **Appliance**, the Appliance  list should be displayed and list all appliances.

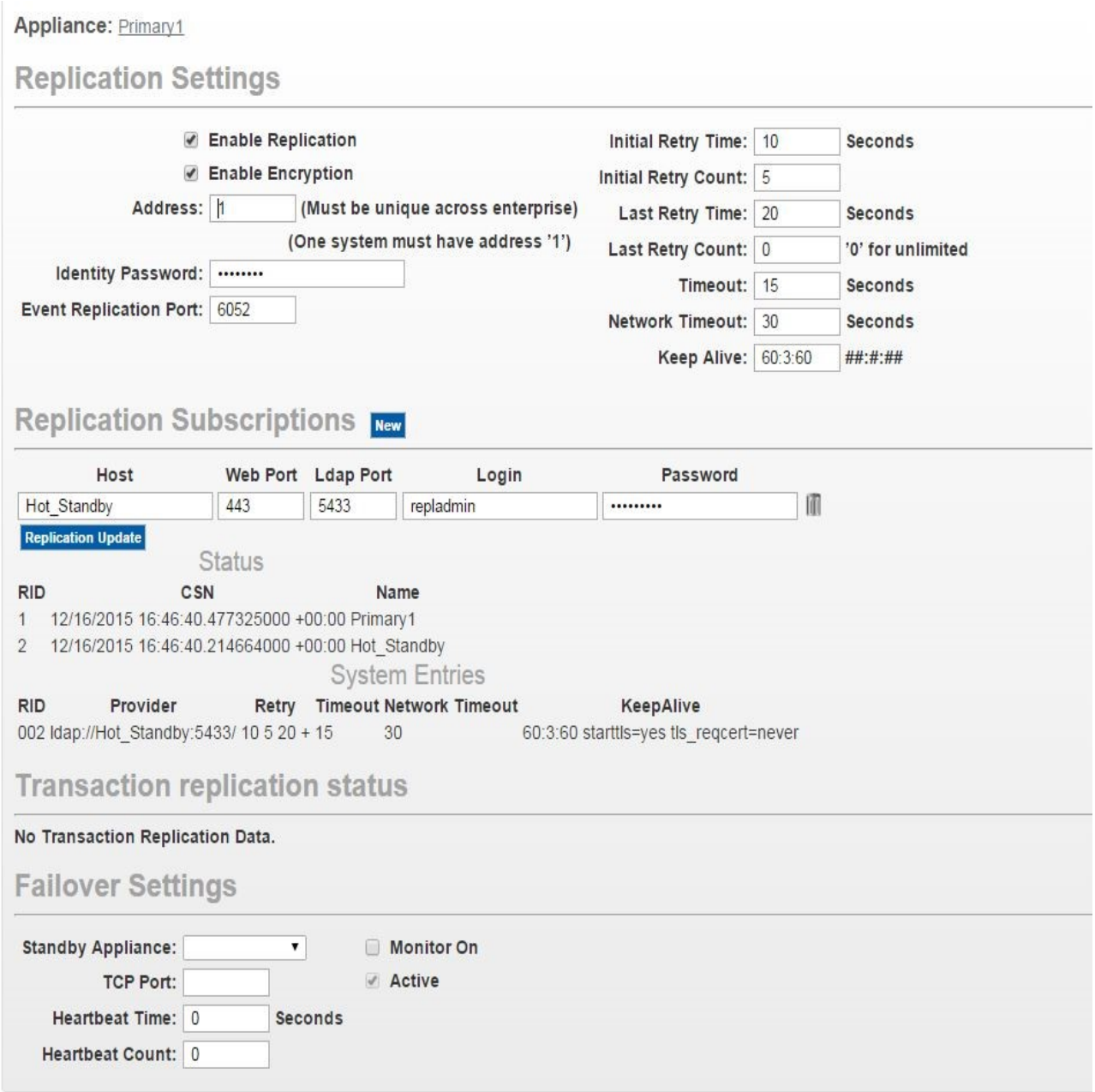



**Figure 12:** Primary Replication tab showing status

### *Testing Two-Way Replication*

1. Make a small change in the primary appliance. For example, update an address for an identity.
2. Access a subscribing appliance and check if you can see the change.
3. Make a small change in the subscribing appliance. For example, update an address for a different identity.
4. Access the primary appliance and check if you can see the change.

If the changes you made appear in both appliances, then replication was set up successfully.

# 4. Setting Up Failover

**Note:** Do not perform this procedure until after replication has been correctly set up. This step assumes that the checkbox for Hot Standby on the Appliance tab has been checked for the appliance serving as the Hot Standby appliance.

1. Log in to the primary appliance. This procedure can only be performed on the primary appliance.
2. In the top-right, select > **Appliance**.
3. Select the primary appliance from the Appliance list.
4. In the Replication tab, enter the following settings in the Failover Settings area:
   a. **Standby Appliance**: Select a standby appliance from the list. You can have more than one standby appliance set up in the system, but only appliances identified as a standby will appear on the list.
   b. **TCP Port**: Enter the primary appliance's TCP port to communicate its health status to the standby appliance.
   c. **Monitor On**: Check this box to turn-on the redundancy monitor. This allows the standby appliance to check the health of the primary appliance and automatically take over if the primary appliance unexpectedly loses network connectivity.
   d. **Heartbeat Time**: Enter how often, in seconds, the secondary appliance should check the health of the primary appliance. If you leave the setting at 0, the system defaults to 60 seconds.

      **Note:** A Heartbeat Count of two and a Heartbeat Time of 30 seconds should typically ensure that a failover is initiated within one to about five minutes of the primary going down. For more information, refer to *Configuring Replication and Failover* on page 327.

   e. **Heartbeat Count**: Enter the number of failures in a row before the secondary appliance takes over for the primary appliance.

      **Tip:** It is recommended to set this to at least two so that a short network glitch does not cause a premature failover.
5. Click to save your changes.

**Appliance:** Primary1

## Replication Settings

- [x] Enable Replication
- [x] Enable Encryption

Address: 1 (Must be unique across enterprise)
(One system must have address '1')

Identity Password: ••••••••

Event Replication Port: 6052

Initial Retry Time: 10 Seconds
Initial Retry Count: 5
Last Retry Time: 20 Seconds
Last Retry Count: 0 '0' for unlimited
Timeout: 15 Seconds
Network Timeout: 30 Seconds
Keep Alive: 60:3:60 ##:#:##

## Replication Subscriptions New

| Host | Web Port | Ldap Port | Login | Password |
|---|---|---|---|---|
| Hot_Standby | 443 | 5433 | repladmin | •••••••• |

Replication Update

### Status

| RID | CSN | Name |
|---|---|---|
| 1 | 12/16/2015 16:57:00.532365000 +00:00 | Primary1 |
| 2 | 12/16/2015 16:57:00.928258000 +00:00 | Hot_Standby |

### System Entries

| RID | Provider | Retry | Timeout | Network Timeout | KeepAlive |
|---|---|---|---|---|---|
| 002 | ldap://Hot_Standby:5433/ | 10 5 20 + 15 | 30 | 60:3:60 | starttls=yes tls_reqcert=never |

## Transaction replication status

| Gateway | Last Trx ID | Last Trx Date | Last Attempt Date | Last Attempt Status |
|---|---|---|---|---|
| Hot_Standby | 95 | 2015-12-16 11:56:36 -0500 | 2015-12-16 11:57:00 -0500 | Success - transferred 2 event records |

## Failover Settings

Standby Appliance: Hot_Standby
TCP Port: 8888
Heartbeat Time: 30 Seconds
Heartbeat Count: 2

- [x] Monitor On
- [x] Active

**Figure 13:** Primary Replication tab, with Hot Standby configured

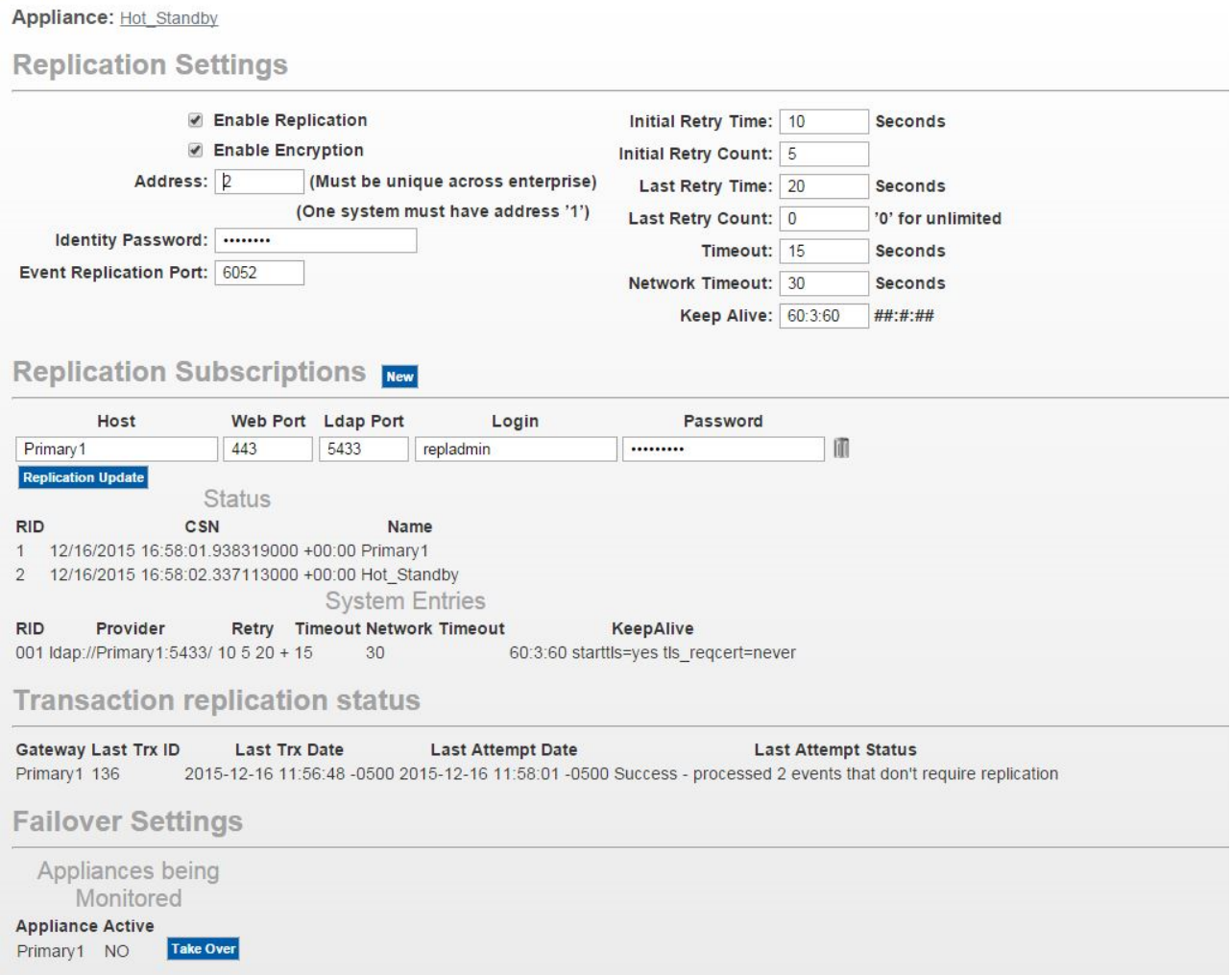



**Figure 14:** Hot Standby replication tab showing Primary being backed up

# Configuring Email Notifications for Replication Events

An event is logged every time a failover or failback occurs. You can configure email to be sent to one or more email addresses whenever a failover and failback event is logged.

The events are:

- Appliance automatic failover completed—After an automatic failover to the Hot Standby appliance this event is logged by the Hot Standby appliance when it is up and running on behalf of the Primary appliance.
- Appliance manual failover completed—After a manual failover this event is logged by the Hot Standby appliance after it is up and running on behalf of the Primary appliance.
- Appliance manual failback completed—After a manual failback this event is logged by the Primary appliance after it is up and running again as the Primary appliance.

Before configuring email notifications for these events:

- Set up and test the SMTP settings configured on both the Primary and Standby appliances.
- Access the Events Listing page and verify that these events are defined.

You can specify the email addresses to which notifications are sent for each event, or you can configure a

custom event type for the three events and specify the email addresses to which notifications are sent for the event type.

1. To specify email addresses to which notifications are sent for each event:
    a. Click **Physical Access** > **Events** to open the Events Listing page and search for the three events. Tip: Search for events containing "Appliance".
    b. Open the first event. The Event: Edit panel opens.
    c. Enter one or more email addresses in the **Email** field. Separate email addresses with commas.
    d. Click .
    e. Repeat for the remaining events.
2. To create an event type for the three events and then specify email addresses to which notifications are sent for the event type:
    a. Click and then Event Types to open the Event Types panel.
    b. Click the **Add Event Type** button. The Event Type: Add panel appears.
    c. Enter a name for the Event type. Complete the other options as required.
    d. Enter one or more email addresses in the **Email** field. Separate email addresses with commas.
    e. Click .
    f. Click **Physical Access** > **Events** to open the Events Listing page and search for the three events. Tip: Search for events containing "Appliance".
    g. Open the first event. The Event: Edit panel opens.
    h. In the **Event Type** option, select the new event type from the drop-down list.
    i. Click .
    j. Repeat for the remaining events.

## Removing Replication and Failover

**Important:** Call Avigilon Technical Support before you attempt to remove or delete the replication and failover settings.

Depending on your system configuration, it may require careful planning before you are able to successfully disable replication and failover on your system. To avoid possible data loss, contact Avigilon Technical Support to help guide you through the process.

## Failing Over and Failing Back

If you've set up replication and failover, the access control system will keep running during planned or unplanned system outages. In the event of a system outage, an appliance may go offline and fail-over to a standby appliance that can take over regular operations until the original appliance comes back online.

In an unplanned system outage, the system will automatically failover. In a planned system outage, you can manually failover an appliance so that the system can continue to run. Once the original appliance is ready to come back online, you can tell the replacement appliance to failback and allow the original appliance to resume normal operations.

## Automatic Failover

If the Monitor On option is enabled in the Primary appliance's Failover Settings area on its Replication tab, the Hot Standby appliance will automatically try to communicate with the Primary appliance periodically. If the Primary appliance does not respond in the set amount of time, the Hot Standby appliance assumes that the Primary appliance has failed, and automatically takes-over for the Primary appliance.

If the Monitor On option is disabled in the appliance's failover settings, the Primary appliance will simply fail and the Hot Standby will not stand-in unless it is manually told to do so.

To check if a Primary appliance has failed-over to a Hot Standby appliance, confirm the following details:

- You are unable to connect to the primary appliance through the web browser.
- When you log in to the Hot Standby appliance, you see that the Hot Standby has started logging hardware events on its Event Monitor screen.

  Hot Standby appliances do not have any connected panels or other hardware until they take over from a Primary appliance, so there should not be any hardware events listed on the Event Monitor screen unless the Hot Standby appliance has stood in for its Primary appliance.
- When accessing the **Appliance** > **Replication** page on the Hot Standby appliance, it is listed as *Active: Yes* beside the name of the inactive Primary appliance.

## Manual Failover

If there is a planned system outage, like an appliance upgrade, you may want to have the primary appliance manually failover to the standby appliance so that the system can continue to function while the upgrade occurs.

In anticipation of a planned system outage, Monitor On failover option should be disabled so that a Primary appliance does not failover until it is instructed to do so.

To manually failover an appliance, complete the following:

1. Log in to the Hot Standby appliance.
2. Access the **Appliances** > **Replication** page.
3. In the Failover Settings area, click the **Take Over** button beside the Primary appliance to instruct the Hot Standby appliance to stand in for the Primary appliance.

After a few moments, the Active status will change to Yes beside the Primary appliance that the Hot Standby has replaced and the Take Over button is replaced by the **Fail Back** button. Notice that once the standby appliance has replaced an appliance, it cannot be set to take over for another Primary appliance until after it has failed back to the Primary appliance that it is standing in for.

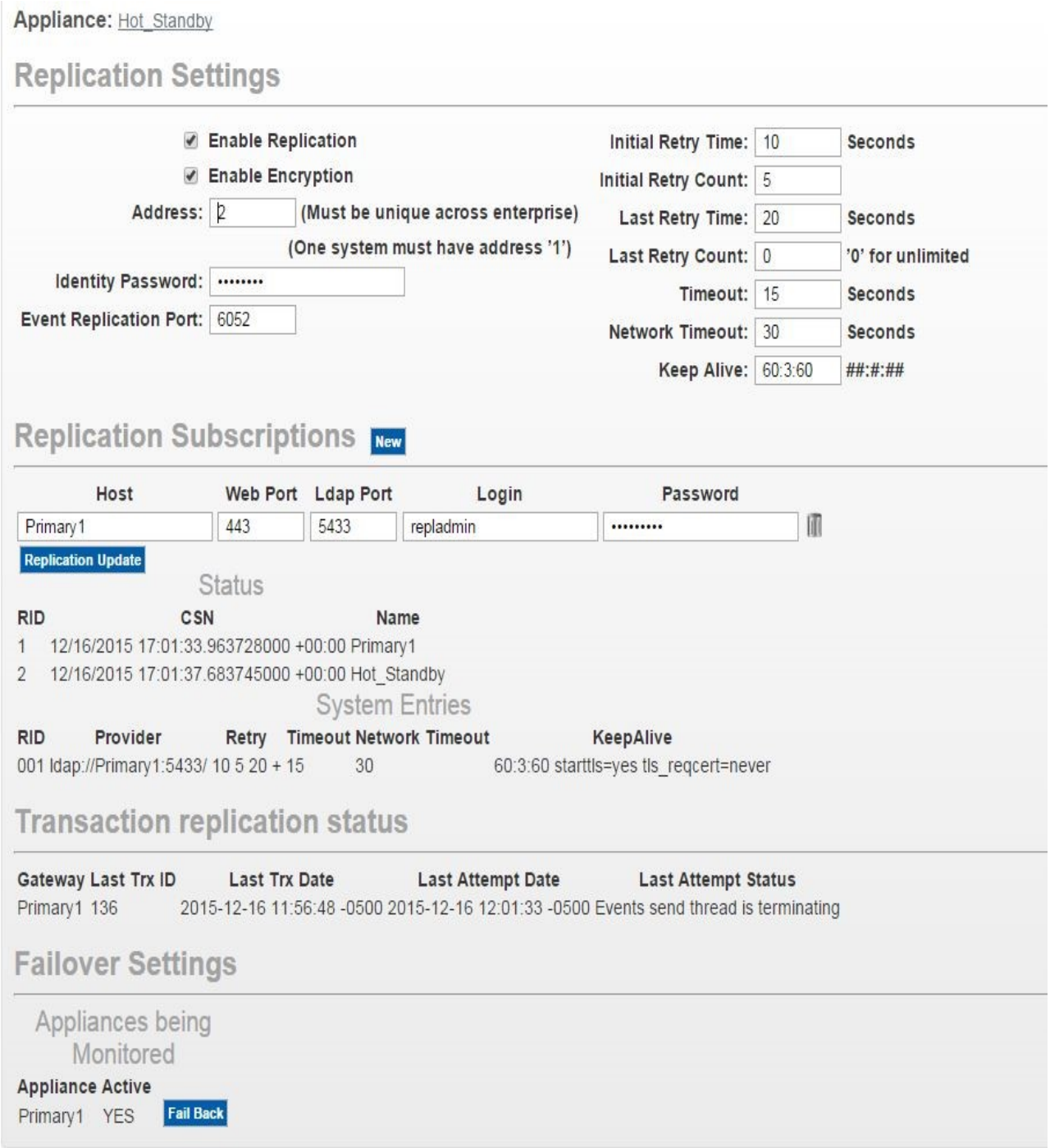



**Figure 15:** Hot Standby after taking over from Primary

## Failback

After a failover has occurred, you can set the standby appliance to failback once the primary appliance is ready to return to normal operations.

1. Log in to the Hot Standby appliance.
2. Access the **Appliances > Replication** page.
3. In the Failover Settings area, click the **Fail Back** button next to the failed over Primary appliance.

### Monitoring Transactional Replication to Hot Standby

As part of the redundancy design, Postgres transactional data is replicated from a Primary appliance to its Hot Standby appliance. This is so that if a failover of the Primary appliance occurs all of the transactional history will be available on the Hot Standby. The status of this replication can be observed for the appliances in the Transaction Replication Status section of the Replication tab on the Appliance: Edit page.

For the Primary appliance, this section contains information about the last row of Postgres transactional data replicated from the Primary to its Hot Standby, including rowid of record in basetrx table (Last Trx ID), date that transaction occurred (Last Trx Date), the last attempted replication time (Last Attempt Time), and its status (Last Attempt Status). For the Hot Standby this information is displayed for the Postgres transactional data it has, with transaction data displayed for the last transaction replicated to the Hot Standby for each Primary it is backing up.

Transaction replication status

| Gateway | Last Trx ID | Last Trx Date | Last Attempt Date | Last Attempt Status |
|---|---|---|---|---|
| Hot_Standby | 99 | 2015-12-16 12:04:23 -0500 | 2015-12-16 12:06:01 -0500 | Success - transferred 2 event records |

**Figure 16:** Primary transaction replication status

Transaction replication status

| Gateway | Last Trx ID | Last Trx Date | Last Attempt Date | Last Attempt Status |
|---|---|---|---|---|
| Primary1 | 157 | 2015-12-16 12:05:50 -0500 | 2015-12-16 12:06:02 -0500 | Success - transferred 17 event records |

**Figure 17:** Hot Standby transaction replication status

# Configuring Network Connections

You can set up how appliances are connected to panels and associated doors. From the Appliance Ports tab, you can set up virtual ports and routes for each Ethernet port. You can also set up serial ports.

## Configuring Ethernet Ports

Appliances can have up to eight RJ-45 Ethernet ports. These high-speed ports can be configured to connect to a series of interlinked door controllers or panels.

> **Note:** You cannot add or remove an Ethernet port from the appliance but you can add virtual ports.

To enable and configure an Ethernet port:

1. From the Appliance Edit page, select the **Ports** tab.
   The Port  list is displayed.
2. Click the name or port number from the Ethernet Ports list.
   The Port: Edit page is displayed.

3. Make the required changes.
4. Click **Save**.

> **Note:** If you assign or change the IP address, make sure that any switches or routers connected to the appliance recognize the changed address. To do this, perform one of the following:

- Reboot the appliance.
- Unplug the Ethernet cable that is connected to the appliance, wait a few seconds, then plug it back in.

If the switch or router is not able to detect the appliance's new IP address, you may need to manually update the switch or router. Refer to the switch or router documentation for more details.

## Adding Ethernet Routes

If you prefer not to use the default Ethernet route set by the appliance, you can add a new Ethernet route for appliance and controller panel communication.

1. From the Appliance Edit page, select the **Ports** tab.
   The Port  list is displayed.
2. In the right most column of the Ethernet Ports list, click **Routes**.
   The Routes  list is displayed.
3. From the Routes  list, click **Add New Route**.
   The Route Add page is displayed.
4. Complete the fields as required to define the new Ethernet route.
5. Click **Save**.
6. Repeat this procedure to add all the routes that are required.

## Enabling Serial Ports

Each appliance includes one or more serial ports for connecting devices via RS-232 or RS-485. Serial ports can be used to connect troubleshooting consoles or to connect panels that do not have Ethernet connections.

To enable a serial port on an appliance:

1. Connect the appliance to one or more panels via the appropriate serial port.
   Note the port number for each serial cable connection.
2. From the Appliance Edit page, select the **Ports** tab.
   The Ports  list is displayed.
3. At the bottom of the page, click the serial port you want to enable.
   The Serial Port Edit page is displayed.
4. Select the **Enable** checkbox.
5. Complete the remaining fields as required to define the serial connection.
6. Click **Save**.

# Backups

You can configure backup events to generate backup files of the configuration and transaction databases of the ACM system. The backup files can be used to restore information if an appliance's configuration or transaction data ever becomes corrupted. They are used to retain data, especially transactional data, for regulatory purposes.

Configuration and transaction data are separately backed up. Backup events can either be scheduled on a daily or weekly frequency, or manually started. Backup files can also be encrypted, which may be required to protect data that is retained for regulatory purposes.

Configuration data, which includes identity information (including photographs, data, and tokens), can generate large backup files. Backups should be generated regularly, and at the very least, following changes. In the event of a catastrophic failure, an up-to-date configuration backup enables the ACM system to be up and running again much faster.

Transactional data, which is generated while the ACM system is active, can be retained in backup form to meet any applicable regulatory requirements, and can be generated to meet data retention policies.

## Backing Up System Data

You can configure the appliance to back up system configuration settings and transaction event details. More than one backup event can be created, and each backup file can be stored in a different location. You can define a schedule for a backup event. Scheduled backups can occur at least once a week or at most once a day at a specific time. A backup event without a schedule must be manually started.

**Note:** Configuration data (including tokens) and transactions data must be backed up separately.

1. From the Appliance Edit page, select the **Backups** tab.
2. Click **Add New Appliance Backup**.

   The Appliance Backup: Add New page is displayed.
3. Enter a name for the back up.
4. Select the preferred **Backup Type**.

   Some of the settings change to match the selected backup type.
5. From the **Data Type** drop down list, select **Configuration** or **Transaction**.
6. Click **Browse** to select where the back up files will be stored.
7. Optionally, in the Schedule area, select the days of the week when the back up will occur then enter the preferred backup time in 24 hour format. Leave the schedule options blank for a backup that can only be manually started.
8. Click **Save**.

## Manually Backing Up Data

After you've set up a backup event, you can manually start a backup at any time; for example, to create a backup of the current data before restoring an older backup.

1. From the Appliance Edit page, select the **Backups** tab.

   The Appliance Backup  list displays.
2. In the row for the backup you want to start, click **Backup Now** to start the backup.

The backup file name is generated in this format: *<backup name>-<date: yyyyMMDDHHMMSS>*.

> **Note:** When you are using the Local Drive backup type, the previous backup file is overwritten. For all other backup types, the file is added to the configured Location.

## Restoring Backups

If the appliance's configuration or transaction data ever becomes corrupted, you can restore the data from a backup.

Start with the most recent backup prior to the data being corrupted. The restored data will overwrite all the configuration or transaction data.

Restored configuration data won't be downloaded to the panels immediately. After the backup is restored, verify that the restored data for panels is correct. For example, identities (or door schedules, or overrides and so on) that you deleted after the backup was created may have to be deleted again, and identities that you added after the backup was created may have to be added again. Then, manually download the restored verified configuration data to each panel in your system. For more information about downloading panels, see *Resetting Doors Connected to a Subpanel* on page 170.

As well as restoring backups from your ACM appliance, you can restore backup files:

- From other ACM systems, or that were created using backup events that are no longer on your system. For more information, see *Restoring Backups From Other Backup Events* below.

  Backups created in versions prior to the ACM software release 5.12.2 may not be compatible with later ACM releases. Contact Customer Support if you need to restore a backup from an earlier release.
- Stored on your local workstation.

To restore a backup file created on your ACM appliance (other than one created by a Local Drive backup event that has been downloaded to the default Downloads folder of your local workstation):

1. From the Appliance Edit page, select the **Backups** tab.

   The Appliance Backup  list displays.
2. Click **File List** beside the backup that you want to restore.
3. In the far right column, click **Restore** beside the copy of the backup that you want to restore.

   The selected file is copied to the appliance and replaces the existing configuration or transaction information on the appliance.

> **Note:** See *Downloading All Tokens* on page 292 if you have restored an ACM appliance that is connected to a SALTO server.

## Restoring Backups From Other Backup Events

You can use a backup event to restore a file created by another backup event, as long as the backup type is the same. This can be useful if you have to restore a backup created with a backup event no longer on your system, or from another ACM system.

**Note:** It is also possible to restore backups from earlier releases of ACM systems. However, backups created in versions prior to the ACM software release 5.12.2 may not be compatible with later ACM versions.

To restore a backup created by another backup event, you must:

1. Identify the name of the backup event used to create the backup:
   a. Locate the backup file that you want to restore. The filename format is *<backup event name>-<date: yyyyMMDDHHMMSS>*.
   b. Note the name of backup event that is embedded in the file name.
2. In the ACM Client software:
   a. From the Appliance Edit page, select the **Backups** tab.

      The Appliance Backup listing page displays.
   b. Rename or create a backup event with the same name as the backup event used to create the backup file:
      - To rename an existing backup event:
        i. Click on the name of the plan to open the Appliance Backup: Edit page.
        ii. Enter the new name for the backup event.
        iii. Leave the other fields as they are.
        iv. Click to save your changes.

        **Tip:** After you have restored the backup file, rename the backup event to its previous name if you want to continue to use it as before.
      - To create a new backup event:
        i. Click to add a new backup event.
        ii. Enter all the details for the backup event, specifying the location of the backup file to be restored.
        iii. Click to save your changes.
3. Copy the backup file to the location specified in the back up event you will use.
4. In the ACM Client software:
   a. Click **File List** beside the backup that you want to restore.

      The Backup File List is displayed.
   b. In the far right column, click **Restore** beside the copy of the backup that you want to restore.

      **Important:** The name of the backup event must match the backup event name embedded in the filename of the backup file.

c. The selected file is copied to the appliance and replaces the existing configuration or transaction information on the appliance.

# Logs

Appliance logs are automatically generated to monitor communications between panels and devices.

## Accessing Appliance Logs

Appliance logs are automatically generated to monitor communications between panels and devices.

The appliance logs are automatically generated and monitor the communications between panels and devices. They can be used to help diagnose appliance issues.

1. From the Appliance Edit screen, select the **Logs** tab.

   The Logs  list is displayed.
2. Click the log you want to view.

   The Appliances Log page displays.

Log details are displayed in chronological order. The earliest log event is displayed at the top, and the most recent is displayed at the bottom. The full text of the log is displayed. Each log is different because of the different activities that are tracked by the log. The name of the Appliance and the Log file are displayed at the top of the screen for each log.

# Software Updates

Software updates are available for download and installation.

## Updating the Appliance Software

Access Control Manager software updates are available for download from the Avigilon website: avigilon.com.

Once you've downloaded the latest version of the software, you can install the update to the appliance from any browser on the network.

1. From the Appliance Edit page, select the **Software Update** tab.

| | |
|---|---|
| **Report Trx backlog** | The count of event transactions waiting to be processed for reporting. |
| **Report Audit backlog** | The count of system and user audit events waiting to be processed for reporting. |
| **File Name** | The name of the update file currently available to this appliance. |
| **Size (Bytes)** | The size of the update file in bytes. |
| **Upload Date** | The time and date when this update file was uploaded to the appliance. |

2. Upload the latest version of the Access Control Manager software to the appliance.
   a. Click **Add Software Update**.
   b. Click **Choose File** and then locate the latest software file that was downloaded.
   c. Click to upload the file to the appliance. It may take several minutes for the upload to complete. Do not navigate away from the page during the upload or the upload is automatically canceled.
3. When the software file is uploaded to the appliance, click next to the filename.
4. When the confirmation message is displayed, click **OK**.

When the update is complete, the appliance will automatically reboot.

**Note:** When the ACM system boots up, you must save the appliance on the Appliance: Edit page to ensure the ACM appliance reboots. You do not need to make any changes to the page prior to clicking Save to have the reboot occur.

# SSL Certificates Overview

For ACM Admin users (default is no delegation) or Super Admin users with the SSL Certificate List, SSL Certificates New, SSL Certificate New CSR and SSL Certificate Load Cert delegations assigned to their role.

A self-signed Secure Socket Layer (SSL) certificate identifies and secures the communication between an ACM appliance, your browser and the external services that interact with the appliance. The appliance certificate and web client certificates will encrypt communication to ensure that only the expected receiver can read the communication.

Update the default self-signed SSL certificate that is shipped with your ACM appliance with your certificate or a certificate provided by your certificate signing authority. ACM allows you to create a new certificate, or create a certificate signing request and then upload it.

**Note:** If you are using FIPS-certified ciphers, ensure the Use FIPS 140-2 compliant ciphers only setting is enabled before you upload a certificate. For more information, see *Enabling FIPS 140-2 Encryption on ACM Appliances* on page 503.

Certificates installed on ACM may affect Allegion Schlage® lock operation, and therefore, must comply with Allegion Schalge lock requirements. For more information, see Schlage documentation. The default web server port in ACM must also be used. If your appliance is using a custom certificate,

Allegion Schlage Wi-Fi locks will require you to upload the proper CA certificate. For more information, see *Step 2: Setting Up Communication to Offline Wi-Fi Locks* on page 277.

## Supported Certificate Standards

The ACM appliance certificate supports the secure hash algorithm, SHA-384 with elliptic curve digital signature algorithm (ECDSA). The SHA-256 with RSA algorithm is still supported for third-party certificates.

**Note:** To provide maximum security strength for your ACM system, ensure the certificate meets the U.S. government's National Institute of Standards and Technology (NIST) Special Publication 800-131A (SP 800-131A) standard.

If your ACM appliance to ACC integration deployment is having trouble connecting, review the certificate requirements for the two systems. You may need to update the certificate on the ACM appliance to resolve the connection issues between the two systems.

## Viewing the SSL Certificate

1. In the top-right, select > **Appliance**.
2. Select the **SSL Certificate** tab.
   The current SSL certificate is displayed.

## Creating an SSL Certificate

To create a self-signed SSL certificate:

1. In the top-right, select >**Appliance**.
2. Select the **SSL Certificate** tab.
3. Click **New Certificate** below the current certificate.

4. Enter:

| | |
|---|---|
| **Country Name** | The two-letter country code. |
| **State or Province Name** | The name of the state or province. |
| **Locality Name** | The locality, such as city. |
| **Organization Name** | The name of your company. |
| **Organization Unit Name** | The unit, section or department. |
| **Common Name** | The hostname of the appliance. |
| **Email Address** | The email address of the support contact in the company. |
| **Subject Alternative Name** | The fully qualified domain name (FQDN) or a comma-separated list of domains, such as `appliance.yourorg.com`, `appliance.yourorg.net`. |
| **Days Valid** | The number of days the SSL certificate is valid for. Range is 1-3650. |

5. Click to save and then **OK** to confirm the certificate creation.

   Your ACM appliance is rebooted automatically to complete the process.

## Creating a Certificate Signing Request

To create a Certificate Signing Request:

1. In the top-right, select >**Appliance**.
2. Select the **SSL Certificate** tab.
3. Click **Certificate Signing Request** below the current certificate.
4. Enter:

| | |
|---|---|
| **Country Name** | The two-letter country code. |
| **State or Province Name** | The name of the state or province. |
| **Locality Name** | The locality, such as city. |
| **Organization Name** | The name of your company. |
| **Organization Unit Name** | The unit, section or department. |
| **Common Name** | The hostname of the appliance. |
| **Email Address** | The email address of the support contact in the company. |
| **Subject Alternative Name** | The fully qualified domain name (FQDN) or a comma-separated list of domains, such as `appliance.yourorg.com`, `appliance.yourorg.net`. |
| **Days Valid** | The number of days the SSL certificate is valid for. Range is 1-3650. |

5. Click .
6. When the **Download CSR** and **Download Private Key** links appear, click them to download both files to your local drive.
7. Send the `certificateRequest.csr` file to your signing authority to obtain a signed certificate.

> **Note:** Protect your `csrPrivatekey.key` file and make sure that it is accessible only to trusted administrators.

Next, see *Uploading an SSL Certificate* below.

## Uploading an SSL Certificate

To upload self-signed certificate files:

1. In the top-right, select >**Appliance**.
2. Select the **SSL Certificate** tab.
3. Click **Load new SSL Certificate**.
4. Upload your new certificate and matching key files from your local drive in the **Upload SSL Certificate** and **Upload Private Key** fields.
5. Click to save and then **OK** to confirm the uploads.

   Your ACM appliance is rebooted automatically to complete the process.

# About Appliances page

View the ACM appliance version and licenses, and add or upgrade licenses, on the **About** tab in > **Appliance**:

## Adding a License

When you first install an ACM 6 system, you will need to license the system to use its features. Add additional licenses to access new features as required.

If you do not already have a license, purchase one from Avigilon.

When adding your first license, you must complete the appliance information on the **Appliance: Edit** page. At a minimum, ACM requires an **Appliance Name** and a **Host Name** to add a license. For information on completing information about the appliance, see *Editing Appliance Settings* on page 326.

### Online Licensing

If you have Internet access, use online activation. Otherwise, see *Offline Licensing* on the next page.

1. In the top-right, select > **Appliance**.
2. In the About tab, click **Add License**.
3. In the Add Licenses dialog, enter your Activation IDs.
   - Click **Add ID** to add additional Activation IDs.
   - Click **Remove Last ID** to clear the last Activation ID entered.
4. Click **Activate Licenses**.

### Offline Licensing

Offline licensing involves transferring files between a computer running the ACM system and a computer with Internet access.

**In the ACM system:**

1. In the top-right, select ⚙ >**Appliance**.
2. In the About tab, click **Add License**.
3. In the Add Licenses dialog, select the **Manual** tab.
4. Enter your Activation IDs.
   - Click **Add ID** to add additional Activation IDs.
   - Click **Remove Last ID** to clear the last Activation ID entered.
5. Click **Save File...** and select where you want to save the `.key` file. You can rename the file as required.
6. Copy the `.key` file to a computer with Internet access.

**In a browser:**

1. Go to activate.avigilon.com.
2. Click **Choose File** and select the `.key` file.
3. Click **Upload**.

   **Important:** When reactivating a site cluster, upload all the deactivation `.key` files first and then the single activation `.key` file at last.

   A `capabilityResponse.bin` file should download automatically. If not, allow the download to occur when you are prompted.
4. Complete the product registration page to receive product updates from Avigilon.
5. Copy the `.bin` file to a computer running the ACC Client software.

**In the ACM system:**

1. In the Add Licenses dialog, click **Choose File**.
2. Select the `.bin` file and click **Open**.
3. Click **Activate Licenses**.

## Removing a License

You can deactivate individual licenses and activate them on a different system.

### Online Licensing

If you have internet access, use the following procedure. Otherwise, see *Offline Licensing* on the next page.

1. In the top-right, select ⚙ >**Appliance**.
2. In the About tab, select the checkboxes next to the licenses you want to remove.

3. Click **Remove License**.
4. Verify the licenses and copy the Activation IDs for your records.
5. Click **Remove Licenses**.

## Offline Licensing

> **Note:** You need a licensing. avigilon.com account. Contact your organization's Technical Contact for access.

Offline licensing involves transferring files between a computer running the ACM system and a computer with Internet access.

**In the ACM system:**

1. In the top-right, select >**Appliance**.
2. In the About tab, select the checkboxes next to the licenses you want to remove.
3. Click **Remove License**.
4. Verify the licenses and copy the Activation IDs for your records.
5. Select the **Manual** tab.
6. Click **Save File...** and select where you want to save the `.key` file.
7. Copy the `.key` file to a computer with Internet access.

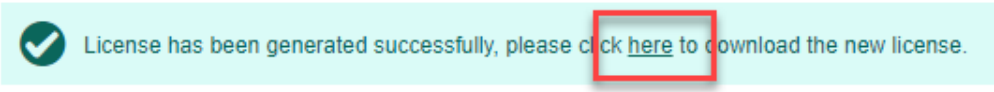
**In a browser:**

   a. Go to activate.avigilon.com.
   b. Click **Choose File** and select the `.key` file.
   c. Click **Upload**.

   > **Important:** When reactivating a site cluster, upload all the deactivation `.key` files first and then the single activation `.key` file at last.

   A `capabilityResponse.bin` file should download automatically. If not, allow the download to occur when you are prompted.
   d. Complete the product registration page to receive product updates from Avigilon.
   e. Copy the `.bin` file to a computer running the ACC Client software.

1. In the success message, click **here** to download the license file `capabilityResponse.bin`.




2. Copy the `.bin` file to a computer running the ACM system.

**In the ACM system:**

1. In the Add Licenses dialog, click **Choose File**
2. Select the `.bin` file and click **Open**.
3. Click **Remove Licenses**.

## Upgrading Your License Format

The ACM 6 license format is different from previous versions. If you upgraded from ACM 5.12.2 to ACM 6.0.0 or later, you will need to upgrade your license format in order to add new licenses. Do not add any new ACM 6 licenses until you have upgraded your old licenses.

> **Note:** If your system is licensed for more than the maximum number of readers, you will not be eligible for an upgrade license. You can continue using your existing system, or contact sales to add more features.

If you do not upgrade your license format, you can continue to use your existing features. However, you will not be able to license new features.

> **Important:** If you use the replication and failover features of the ACM system and you choose to upgrade the license format you must upgrade the license format on both the primary and standby ACM appliances. Replication features, including failover, will not function if the license format is not the same on both appliances. Complete the following steps on both appliances.

1. In the top-right, select >**Appliance**.
2. In the About tab, click **Download Upgrade File**.
3. Email the `.bin` file to acm.license@avigilon.com. You will receive a response in 1-2 business days with an Activation ID for each feature you have. You can continue to use the ACM appliance during this time.
4. After you receive the Activation IDs, follow the procedure in *Adding a License* on page 357. You will only need to enter one of the Activation IDs to automatically license the system for all features your device is entitled to.

## Viewing the End User License Agreement

Follow the steps below to view the End User License Agreement:

1. In the top-right, select > **Appliance**.
2. In the About tab, click **View End User License Agreement Terms and Conditions**.
3. Click **Back** to return to the Appliance: Edit page.

## About Appliances page

View the ACM appliance version and licenses, and add or upgrade licenses, on the **About** tab in > **Appliance**:

| | |
|---|---|
| **Appliance Name** | The name of the appliance. |
| **Application Software Version** | The current software version running on the appliance. |
| **Database Version** | The current database version running on the appliance. |
| **End User License Agreement Status** | Whether the terms and conditions have been accepted. |
| **View End User License Agreement Terms and Conditions** | Click to review the software end user license agreement. |
| **Licenses** | |
| **Add License** | Click to add licenses to the system. |
| **Remove License** | Click to remove licenses from the system. |
| **Counts** | The number of readers, panels, wireless locks, and ACM system integrations that are licensed to the appliance. |
| **External Systems** | The external vendors that are licensed to run with the appliance. |
| **Collaborations** | The external information sources that are licensed for the import and export of ACM identity information. |
| **Options** | The features the appliance supports. |

# Managing Collaborations

Connect, customize and set up your appliance to meet your system requirements. Possible functions include:

- Pulling identity information from an external database to populate identity fields in the Access Control Manager.
- Pushing identities and events from the Access Control Manager to third-party applications such as video management software.

**Note:** Any date fields in Collaboration files (e.g. Last Access, Expire Date, Activate Date, Issue Date) will display as blank if there is no information recorded for that field. The Force Password Change and MFA Device fields do not apply to collaborations.

**Important:** After upgrading to ACM 6.50 or later, you must re-trust your SSL certificates for external domains and identity LDAP pull collaborations before users authenticated by those mechanisms can access ACM. Only systems with uploaded certificates have trust maintained after the upgrade. This does not apply to implementations that do not use SSL certificates or do not have external domains or identity LDAP pull collaborations. For more information, see *Re-trust Certificates* on page 398.

## Adding a Collaboration

For the types of collaboration available in the ACM application, see *Supported Collaborations* on page 369.

To add a collaboration:

1. Select > **Collaboration**.

   The Collaborations list appears.
2. Click **Add Collaboration**.

   The Collaboration Add New page appears.
3. Fill out the **Name**, **Appliance** and **Type** fields. Depending on the type of collaboration selected, additional fields will display.
4. Select the **Installed** checkbox to enable the collaboration.
5. Complete the remaining fields as required. The fields will vary depending on the collaboration type:

| Collaboration type | Additional fields |
|---|---|
| Events - Generic XML; Events - Splunk | Host; Port Number; Require TCP |

| | |
|---|---|
| Identity CSV Export | Partitions (if configured); Partitions to Export (if configured); Include Primary Photo; Include Roles; Location Type; and for SCP or Windows Share only: Host, Port Number, User Name, Password, Location, Domain Name (Windows Share only)<br><br>**Note:** Only one Local Drive Identity CSV Export collaboration is allowed. You can update the definition of the existing collaboration, or replace it with a new one by manually deleting the existing one and adding a new one. For more information, see *Deleting a Collaboration* on page 373. |
| Identity CSV one-time Long format | Delimiter; Text Qualifier; Date Format; CSVFile |
| Identity CSV one-time Short format | CSVFile |
| Identity CSV Recurring | Include Primary Photo; Location Type; Host; Port Number; User Name; Password; Location; Delimiter; Text Qualifier; Date Format; Domain Name (Windows Share) |
| Identity LDAP pull | Host; Bind DN; Password: Port Number; SSL, Validate Certificate |
| Identity Oracle RDBMS pull | Host; User Name; Instance; Port Number; Password |
| Identity SQL Server pull | Host; User Name; Database; Port Number; Password<br><br>**Note:** Ensure any individual images to be imported are not over 1MB. |

6. Click **Save**.
   The Collaboration: Edit screen appears.
7. Navigate through the tabbed pages and fill out the details as required.
8. Click **Save**.

## Adding an Events XML Collaboration

**Note:** The ACM license, AC-SW-LIC-XML, is required to enable this feature.

To add an Events XML collaboration:

1. Select > **Collaboration**.

   The Collaborations list appears.
2. Click **Add Collaboration**.

   The Collaboration: Add page appears.
3. Complete the following fields:

| | |
|---|---|
| **Name** | Name for the collaboration. |
| **Appliance** | Select the appropriate Appliance, if more than one appliance is available. |
| **Type** | Select Events – Generic XML.<br>The following additional fields display once the type is selected:<br>• Host<br>• Require TCP<br>• Port Number |
| **Installed** | Select this checkbox to enable the collaboration. |
| **Host** | IP address of the XML receiver. |
| **Require TCP** | Select this checkbox. |
| **Port Number** | TCP port relating to the Host IP address. |

4. Click **Save**.

   The message 'Collaboration entry was successfully created' displays on the Collaboration: Edit screen.
5. Click the **Events** tab.
6. Complete the following fields:

| | |
|---|---|
| **Schedule** | Select a Schedule for when the XML events collaboration will be active. |
| **Send Acknowledgments** | Select this checkbox to include acknowledgments. |
| **Send Clears** | Select this checkbox to include clears. |
| **Send Notes** | Select this checkbox to include notes created by Alarm Monitor operators when processing alarms. |

7. Select the desired event types to be included in the XML data feed from the **Available** list and move them to the **Members** list.

   **Note:** Hold the SHFT key down and select the first and last entries to select multiple consecutive entries. Hold the CTRL key down to select multiple non-consecutive entries.

8. Click **Save**.

## Collaborations - Events XML Definitions

Definitions for the individual attributes of the XML events stream are noted below:

To see a typical example, refer to *Collaborations - Events XML Example* on page 367.

| XML | Definition |
|---|---|
| <plasectrxGatewayDN> cn=544de4aa06914073,ou=gateways ,dc=plasec </plasectrxGatewayDN> | An internal reference for the ACM appliance that this XML came from. |
| <cn>38901f4a95d14013</cn> | The unique row identifier for this particular event. Corresponds to the ID column in the history tables. |
| <plasectrxRecdate>20140610055028-0700 </plasectrxRecdate> | Time the event was logged into the ACM system history – adjusted for ACM local time. |
| <plasectrxPanel date>20140610085028-400 </plasectrxPanel date> | The UTC time the event actually happened. It is the timestamp of the event being reported up from the field hardware. Adjusted for field hardware local time. |
| <plasectrxRecdateUTC>20140610125028Z </plasectrxRecdateUTC> | Time the event was logged into the ACM system history. |
| <plasectrxPanel dateUTC>20140610125028Z </plasectrxPanel dateUTC> | The UTC time the event actually happened. It is the timestamp of the event being reported up from the field hardware. |
| <plasectrxLastacc> 19700101000000Z</plasectrxLastacc> | Last Access time and date of the Token that is associated with this event. Example – the last recorded valid access of the card that was used at a door causing a 'Local Grant' event. |
| <plasectrxEvtypename> Intrusion</plasectrxEvtypename> | ACM event type category for this event. Corresponds to one of the event types defined in the ACM system in Settings: Event Types. |
| <plasectrxBackgroundColor> </plasectrxBackgroundColor> | Color assigned to the event background color (if any) for display in the ACM monitor. |
| <plasectrxForegroundColor> </plasectrxForegroundColor> | Color assigned to the event foreground color (if any) for display in the ACM monitor. |
| <plasectrxAckBackgroundColor> </plasectrxAckBackgroundColor> | Color assigned to the event background color (if any) for display in the ACM monitor. This color corresponds to an 'acknowledged alarm' on the Alarms page. |
| <plasectrxAckForegroundColor> </plasectrxAckForegroundColor> | Color assigned to the event foreground color (if any) for display in the ACM monitor. This color corresponds to an 'acknowledged alarm' on the Alarms page. |
| <plasectrxEventname> Input point in alarm </plasectrxEventname> | Name of the event. Corresponds to one of the events defined in the ACM system in Physical Access: Events. |
| <plasectrxPanel name>elevator test </plasectrxPanel name> | Name of the panel that the event originated from. |
| <plasectrxSourcename> Input on subpanel 0 Address 1 </plasectrxSourcename> | Name of the source of the event. |
| <plasectrxSourcelocation> </plasectrxSourcelocation> | Location of the source of the event, as defined in the 'Location' field on the various hardware property pages. |

| XML | Definition |
|---|---|
| <plasectrxSourcealtname> </plasectrxSourcealtname> | Applies to doors only - if the event source is a door, this is the Alt. Name as defined on the Door properties Configuration tab. |
| <plasectrxPointaddress> 750</plasectrxPointaddress> | A reference number for the event e.g. 'Input point in alarm'. |
| <plasectrxPointDN> cn=750,ou=points,dc=plasec </plasectrxPointDN> | This is the LDAP dn of the 'Input point in alarm' event, for lookup during ACM processing. |
| <plasectrxEvtypeaddress>5 </plasectrxEvtypeaddress> | This is a reference number for the event type e.g. 'Intrusion'. |
| <plasectrxSourceDN> cn=100,cn=0,cn=9,ou=panels, cn=544de4aa06914073,ou=gateways, dc=plasec </plasectrxSourceDN> | LDAP dn of the source of the event, used in ACM processing. |
| <plasectrxSourcetype>40 </plasectrxSourcetype> | An internal reference to the type of hardware the event source belongs to. Defines what type of hardware produced the event – an input point in this case. |
| <plasectrxOperatorname> </plasectrxOperatorname> | the ACM system operator that is associated with certain events e.g. an audit event for a record updated by an the ACM system user. |
| <plasectrxPri>10</plasectrxPri> | Priority of the event, as defined on the Event properties page. |
| <plasectrxMsg></plasectrxMsg> | Contents of the 'Message' column in the Monitor e.g. the raw card data from an 'Invalid Card Format' event. |
| <plasectrxIdentityDN> </plasectrxIdentityDN> | The LDAP dn of the identity associated with the event. Example – the dn of the identity that used their card at a door causing a 'local grant' event. |
| <plasectrxCardno>0 </plasectrxCardno> | Internal number of the token that is associated with this event. Example – the card number that was used at a door causing a 'local grant' event. |
| <plasectrxEmbossedno> </plasectrxEmbossedno> | Embossed number of the token that is associated with this event. Example – the card number that was used at a door causing a 'local grant' event. |
| <plasectrxLname> </plasectrxLname> | Last name of the identity associated with the event. Example – the last name of the identity that used their card at a door causing a 'local grant' event. |
| <plasectrxFname> </plasectrxFname> | First name of the identity associated with the event. Example – the first name of the identity that used their card at a door causing a 'local grant' event. |
| <plasectrxMi></plasectrxMi> | Middle name of the Identity associated with the event. Example – the middle name of the identity that used their card at a door causing a 'local grant' event. |

| XML | Definition |
|---|---|
| <plasectrxIssuelevel>-1 </plasectrxIssuelevel> | Issue level of the token that is associated with this event. Example – the issue level of the card that was used at a door causing a 'local grant' event. |
| <plasectrxFacilityCode>0 </plasectrxFacilityCode> | Facility code of the token that is associated with this event. Example – the facility code of the card that was used at a door causing an 'invalid facility code' event. |
| <plasectrxExpiredat> 19700101000000Z </plasectrxExpiredat> | Deactivate date of the token that is associated with this event. Example – the deactivate date of the card that was used at a door causing a 'local grant' event. |
| <plasectrxActivdat> 19700101000000Z </plasectrxActivdat> | Activate date of the token that is associated with this event. Example – the activate date of the card that was used at a door causing a 'local grant' event. |
| <plasectrxIssuedat> 19700101000000Z </plasectrxIssuedat> | Issue date of the token that is associated with this event. Example – the issue date of the card that was used at a door causing a 'local grant' event. |
| <plasectrxHasCamera>0 </plasectrxHasCamera> | Indicates whether the event has a camera view associated with it. Used in the monitor to display the camera icon for an event with a camera association. |
| <plasectrxHasNotes>0 </plasectrxHasNotes> | Indicates whether there are any notes available for this event. |
| <plasectrxHasSoftTriggerSet>0 </plasectrxHasSoftTriggerSet> | Indicates whether there is a soft trigger associated – currently this applies to Exacq video integration only. |
| <plasectrxShowVideo>0 </plasectrxShowVideo> | Indicates whether the event is optioned to show pop-up video of an associated camera. |
| <plasectrxSeqno>0 </plasectrxSeqno> | Not used. |
| <plasectrxIsAlarm>1 </plasectrxIsAlarm> | Indicates whether this event is also defined as an alarm. Alarms appear on the Monitor: Alarms page. |

## Collaborations - Events XML Example

Shown below is an example of a typical 'input point in alarm' XML events stream:

```
<EVENT>

    <plasectrxGatewayDN>cn=544de4aa06914073,ou=gateways,dc=plasec</plase
    ctrxGatewayDN>

    <cn>38901f4a95d14013</cn>

    <plasectrxRecdate>20140610055028-0700</plasectrxRecdate>

    <plasectrxPanel date>20140610085028-0400</plasectrxPanel date>

    <plasectrxRecdateUTC>20140610125028Z</plasectrxRecdateUTC>
```

```
<plasectrxPanel dateUTC>20140610125028Z</plasectrxPanel dateUTC>

<plasectrxLastacc>19700101000000Z</plasectrxLastacc>

<plasectrxEvtypename>Intrusion</plasectrxEvtypename>

<plasectrxBackgroundColor></plasectrxBackgroundColor>

<plasectrxForegroundColor></plasectrxForegroundColor>

<plasectrxAckBackgroundColor></plasectrxAckBackgroundColor>

<plasectrxAckForegroundColor></plasectrxAckForegroundColor>

<plasectrxEventname>Input point in alarm</plasectrxEventname>

<plasectrxPanel name>elevator test</plasectrxPanel name>

<plasectrxSourcename>Input on subpanel 0 Address
1</plasectrxSourcename>
<plasectrxSourcelocation></plasectrxSourcelocation>

<plasectrxSourcealtname></plasectrxSourcealtname>
<plasectrxPointaddress> 750</plasectrxPointaddress>

<plasectrxPointDN>cn=750,ou=points,dc=plasec</plasectrxPointDN>

<plasectrxEvtypeaddress> 5</plasectrxEvtypeaddress>

<plasectrxSourceDN>cn=100,cn=0,cn=9,ou=panels,cn=544de4aa06914073,ou
=gateways,dc=plasec
</plasectrxSourceDN>

<plasectrxSourcetype>40</plasectrxSourcetype>

<plasectrxOperatorname></plasectrxOperatorname>

<plasectrxPri>10</plasectrxPri>

<plasectrxMsg></plasectrxMsg>

<plasectrxIdentityDN></plasectrxIdentityDN>

<plasectrxCardno> 0</plasectrxCardno>

<plasectrxEmbossedno></plasectrxEmbossedno>

<plasectrxLname></plasectrxLname>

<plasectrxFname></plasectrxFname>

<plasectrxMi></plasectrxMi>

<plasectrxIssuelevel> -1</plasectrxIssuelevel>

<plasectrxFacilityCode>0</plasectrxFacilityCode>

<plasectrxExpiredat>19700101000000Z</plasectrxExpiredat>

<plasectrxActivdat>19700101000000Z</plasectrxActivdat>
```

```
    <plasectrxIssuedat>19700101000000Z</plasectrxIssuedat>
    <plasectrxHasCamera>0</plasectrxHasCamera>
    <plasectrxHasNotes>0</plasectrxHasNotes>
    <plasectrxHasSoftTriggerSet>0</plasectrxHasSoftTriggerSet>
    <plasectrxShowVideo>0</plasectrxShowVideo>
    <plasectrxSeqno>0</plasectrxSeqno>
    <plasectrxIsAlarm>1</plasectrxIsAlarm>
</EVENT>
```

For definitions of the individual attributes, refer to *Collaborations - Events XML Definitions* on page 364.

# Editing a Collaboration

To edit an existing collaboration:

1. Select > **Collaboration**.
   The Collaborations list appears.
2. Click on the name of the collaboration you want to edit.
   The Collaboration Edit screen appears.
3. Navigate through the tabbed pages and make the required changes.
4. Click **Save**.

# Supported Collaborations

> **Note:** Up to 32 collaborations—in any combination by Type or Installed status—are supported by an ACM appliance.

The types of collaboration available in the ACM application include:

| Type | Description |
|---|---|
| **Identity** | |
| **Identity CSV Export** | Export identities, photos, tokens, groups, and roles to a CSV file.<br>**Note:** Only one Local Drive Identity CSV Export collaboration is allowed. |

| Type | Description |
|---|---|
| **Identity CSV One-time Long format** | Import identities, tokens, groups, roles from a CSV file manually and keep the Access Control Manager identity database in sync with changes. |
| **Identity CSV One-time Short format** | Import identities, tokens, groups, roles from a CSV file manually and keep the Access Control Manager identity database in sync with changes. |
| **Identity CSV Recurring** | Import identities, photos, tokens, groups, and roles from an updated CSV file and keep the Access Control Manager identity database in sync with changes. |
| **Identity LDAP pull** | Pull identities, tokens, groups, roles from a directory store and keep the Access Control Manager identity database in sync with changes. |
| **Identity Oracle RDBMS pull** | Pull identities, tokens, groups, roles from a Oracle RDBMS store and keep the Access Control Manager identity database in sync with changes. |
| **Identity SQL Server pull** | Pull identities, tokens, groups, roles from a Microsoft SQL Server RDBMS store and keep the Access Control Manager identity database in sync with changes.<br><br>**Note:** Microsoft SQL Server 2005 or newer is required. |
| **Events** | |
| **Events - Generic XML** | Transmit events in real time using XML. |
| **Events - Splunk** | Produces messages in Splunk format. Splunk is a log aggregation product. |

# Running a Collaboration

To run a collaboration:

1. Select > **Collaboration**.

   The Collaborations list appears.
2. Click from the **Run** column next to the collaboration you want to run.
3. When the confirmation message is displayed, click **OK**.

   Allow more time for the collaboration to run if you are using the SCP or Windows Share location type. Running the Local Drive location type is faster because network performance is not a consideration.
4. View the ACM identity and token information as follows:

   **Note:** The maximum file size recommended for unzipped information is 25GB. This maximum equates to approximately 12,500 identities if each identity has a 2MB photograph, or 6,250 identities if each identity has a 4MB photograph.

- For previews of Identity CSV Recurring, Identity LDAP pull, Identity Oracle RDBMS pull and Identity SQL Server pull collaborations in the general log, see *Previewing the General Identity Collaboration Log* below.
- For exports to SCP or Windows Share network locations, view the files (unzipped) in the location specified in the collaboration.
- For exports to Local Drive, click when it appears and view the contents of the zipped CSV export file. See *Extracting a CSV Zip File* on the next page.

# Previewing the General Identity Collaboration Log

You can click the Preview icon to view the general log for identity collaborations that were run, when each collaboration was started, how long each collaboration took to complete in minutes, the number of identities that were exported and the compression level (deflate format) of each item. Recent entries are shown at the top of the log, and older entries at the end of the log. For information about accessing the individual logs, see *Accessing Appliance Logs* on page 353.

The general identity collaboration log can be previewed for these types of collaborations:

- Identity CSV Recurring
- Identity LDAP pull
- Identity Oracle RDBMS pull
- Identity SQL Server pull

The following examples show an Identity CSV Export to Local Drive collaboration and a previewed log in the Identity Collaboration Log....

**Figure 18:** Example of two collaborations that were run and completed

20191024-010540 collab_idfile:<Vancouver Appliance> 2019 10/24 01:05:40-0700 **********STARTING COLLABORATION RUN.**********

20191024-010540 collab_idfile:<Vancouver Appliance> Running Export Collaboration...

==========

Started at: 2019-10-24 01:05:56 -0700

Finished at: 2019-10-24 01:13:59 -0700

Total timing: 483.713355605

Total Identities Exported: 10106

==========

adding: ACM_identity_export.csv (deflated 81%)

adding: ACM_manifest.yml (deflated 58%)

adding: photos/ (stored 0%)

adding: photos/caa41a44-8a46-1039-8dbe-7178c5f2b90a.jpg (deflated 0%)

adding: photos/51a4f380-8a45-1039-92bf-7178c5f2b90a.jpg (deflated 2%)

...

20191024-073545 collab_idfile:<Vancouver Appliance> 2019 10/24 07:35:45-0700 **********ENDING COLLABORATION RUN.**********

**********STARTING COLLABORATION RUN.**********

20191024-083545 collab_idfile:<Vancouver Appliance> Running Export Collaboration...

==========

Started at: 2019-10-24 08:36:05 -0700

Finished at: 2019-10-24 08:44:13 -0700

Total timing: 487.375753767

Total Identities Exported: 10106

==========

adding: ACM_identity_export.csv (deflated 81%)

adding: ACM_manifest.yml (deflated 58%)

adding: photos/ (stored 0%)

...

**Figure 19:** Example of a previewed collaboration

20191029-213702 collab_idfile:<Vancouver Appliance 5> 2019 10/29 21:37:02+0000 **********STARTING COLLABORATION RUN - preview only mode.**********

20191029-213702 collab_idfile:<Vancouver Appliance 5> Obtaining input file(s)...

Transfer using NAS - CIFS

...

20191031-000839 collab_idfile:<Vancouver Appliance 5> 2019 10/31 00:08:39+0000 **********ENDING COLLABORATION RUN - preview only mode.**********

# Extracting a CSV Zip File

To extract a zipped comma delimited (CSV) file that contains exported ACM identities and tokens:

**Note:** The 7-Zip tool is recommended for extracting zipped CSV export files larger than 4GB. The maximum file size recommended for unzipped information is 25GB. This maximum equates to approximately 12,500 identities if each identity has a 2MB photograph, or 6,250 identities if each identity has a 4MB photograph.

1. Select > **Collaboration**.
   The Collaborations list appears.
2. Click next to **Local Drive** for the collaboration that was run.
3. The `collaboration_name-yyyymmddhhmmss.zip` file is downloaded to the local drive on an ACM appliance. The `hh` value is specified in 24-hour format.

4. Extract and examine the contents:
   - `photos` folder contains the photographs of the exported identities.
   - `ACM_manifest.yml` provides:
     - `source`: The name of the appliance.
     - `software version`: The version of the ACM software.
     - `db_version`: The version of the ACM, LDAP or appliance configuration database.
     - `assets: ACM_identity_export.csv`: The identifier of the CSV export file.
   - `ACM_identity_export.csv` spreadsheet provides exported ACM identity and token information in columns A through AL. See the following sample:

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Export UUID | External System ID | Status | Type | ID Modify Time | Load Date | Partition | First Name | Last Name | Middle Name | Address | City | State | Zip | Phone | Work Phone | Email Address | Title |
| 2 | 4713cd90-8a4 | a4cdeccc-1ea8-1035- | 1 | Janitor | 10/24/2019 01:1 | 04/19/2013 07:00:00Z | | Steve | Lee | | 1234 Strawberry | Palo Alto | California | 94301 | 650-123-4567 | 650-234-5678 | slee@company.com | Facilities Manager |
| 3 | a15ef250-8a4 | 4bb8a216-12d3-1035 | 1 | Long Term Guest | 10/24/2019 00:5 | 06/05/2012 07:00:00Z | | Justin | Smith | | 5678 Main Street | Palo Alto | California | 94303 | 650-890-1234 | 650-234-5678 | jsmith@consulting.com | Support Engineer |
| 4 | e80defa6-8a4 | 98344adc-1ea4-1035- | 1 | Employee | 10/24/2019 01:1 | 06/06/2012 07:00:00Z | | Katie | Forest | | 9012 Second Ave | Palo Alto | California | 94303 | 650-567-8901 | 650-234-5678 | kforest@company.com | Support Analyst |

> **Note:** The VIP column refers to the anti-passback (APB) setting.

# Deleting a Collaboration

To delete an existing collaboration:

1. Select > **Collaboration**.
   The Collaboration list appears.
2. Click beside the collaboration that you want to delete.
3. When the confirmation message is displayed, click **OK**.

# Assigning an Event Type to a Collaboration

To assign an event type to a collaboration:

1. Select > **Collaboration**.
2. From the Collaboration list, click on the name of the collaboration you want to edit. It must be an Event collaboration type.
   The Collaboration Edit screen appears.
3. Select the **Events** tab.
4. From the Available list, select all the events you want to transfer, then click .
   The event is added to the Members list to show that it is now assigned.

   To remove an event from the collaboration, select the event from the Members list, then click .

> **Note:** You can select multiple events by using the **Ctrl** or **Shift** key.

5. Click **Save**.

# Setup & Settings

Click or hover over ⚙ in the upper-right corner to:

- **Appliance** — Connect, customize and set up your appliance to meet your system requirements. For more information, see *Managing Appliances* on page 326.
- **Collaboration** — Set up and manage collaborations which exchange data with third-party databases and applications. For more information, see *Managing Collaborations* on page 362.
- **Schedules** — Configure when a door is accessible, when a card is valid, or when a device is activated.
- **Holidays** — Configure dates when normal rules are suspended in schedules.
- **Event Types** — Configure event types and instructions on how to handle the event generated in the ACM system. For more information, see *Event Types* on page 381.
- **User Forms** — Customize the identity and tokens tabs or create additional ones, and then assign them to ACM operators. For more information, see *User Forms Overview* on page 385.
- **User Fields** — Add additional fields for enrolling identities. For more information, see *User Defined Fields* on page 387.
- **User Lists** — Add additional drop-down option lists for enrolling identities. For more information, see *User Lists* on page 389.
- **System Settings** — Configure system settings such as language, token expiration time, required password strength and more. For more information, see *System Settings* on page 390.
- **Paired Devices** — Generate a one-time key to connect a browser-enabled device, such as a smartphone, to a door configured as an ACM ACM Verify station so that it can function as a Virtual Station. For more information, see *Paired Devices* on page 263.
- **Certificates** — Mercury controllers only. Add custom certificates for panel and ACM authentication.
- **Badge Designer** — Customize a badge template for badge holders. For more information, see *Badge Templates and the Badge Designer* on page 403
- **External Systems** — Set up integration to cameras, sites and other third-party external systems. For more information, see *External Systems* on page 409.
- **Maps** — Import maps of your facility and populate them with door, panel, subpanel, input, output, camera and global action alarm points that can be monitored. For more information, see *Maps* on page 429.

## Schedules and Holidays

### Schedules

A schedule controls when a door setting is active. For example, you can apply a schedule to a group of users and secured doors to grant and deny access to the days and times specified in the schedule.

A door can be assigned an 'unlock schedule', which specifies a period of time when no credential is required to access the door. All users have free access during the 'unlock schedule' period. Likewise, a device may be assigned an 'active schedule', a period during which the device is in operation.

You can also create a holiday list to manage access during holidays or special days when the building is closed. Before you can create a schedule to handle special occasions, you must set up the holiday list.

For more information, see:

- *Searching for Schedules* below
- *Adding Schedules (Intervals in Schedules)* on the next page
- *Editing Schedules* on page 378
- *Deleting Schedules* on page 378

When a panel is not operating as expected, see *Panel Events* on page 500 for troubleshooting instructions.

## Holidays

Holidays are special days in the year when the standard schedule does not apply or a different entry and exit pattern is observed. New Year's Day and National Day are examples of holidays. The Access Control Manager is designed to accommodate a large number of diverse holidays.

> **Note:** Holidays are set for a specific day in the year. You need to update the system holidays each year.

For more information, see:

- *Adding Holidays* on page 379
- *Editing Holidays* on page 380
- *Deleting Holidays* on page 380
- *Examples* on page 380

## Searching for Schedules

View all the schedules that have been configured in the ACM system on the **Setup & Settings** > **Schedules** page.

To narrow down the search results:

1. Select **Name**, **Mode**, or **Partitions** in **Search Field**.

   **Partitions** is displayed only if partitions are defined in your ACM system.
2. Select the search operator in **Search Value** and your search criteria.
3. Optional. To refine your search, click **Add Criteria**, repeat the above steps, and select the **And** or **Or** search operator (located next to the Search button).

   To remove a single criteria row, click **Remove**. To clear all fields, click **Clear Search**.
4. Click **Search**.

The results are displayed.

| | |
|---|---|
| **Name** | The name of the schedule.<br>Click the name to edit the schedule. |

| | |
|---|---|
| **Mode** | The mode of the schedule.<br>• ON – The schedule is constantly on. You do not need to set specific dates or times for the schedule.<br>• OFF – The schedule is constantly off.<br>• SCAN – The schedule follows the date and time set in the checkboxes. |
| **Delete** | Click to delete the schedule. |
| **Add Schedule** | Click the button to create a new schedule. |
| **Create New Report** | Click the button to generate a report of all the schedules in the system. |

## Adding Schedules (Intervals in Schedules)

1. Select > **Schedules**.

   The two default 24 Hours Active (ON) and Never Active (OFF) schedules cannot be deleted.
2. Click **Add Schedule**.
3. Enter a name for the schedule in **Name**.
4. Edit the **Advanced Schedules** field, if needed: The checkbox is checked by default for new schedules and any existing schedules that were previously configured using the advanced capability (at time of initial release of the field).
   - If checked, you can apply different selections of holidays to the intervals in the schedule. (The page refreshes and displays columns of holiday checkboxes.)
   - If unchecked, you can apply the same selection of holidays to the schedule itself. (The page refreshes and displays a single row of holiday checkboxes.)

   **Note:** The Advanced Schedule option is not supported for ASSA ABLOY IP doors.
5. Select the schedule mode:
   - **ON** – The schedule is constantly on. You do not need to set specific dates or times. Click to save the new schedule.
   - **OFF** – The schedule is off. Click to save the new schedule.
   - **SCAN** – The schedule follows a weekly, monthly or shift rotation and includes any holidays. One interval is represented by one row of checkboxes.

     For **SCAN** mode:

     a. Click the days of the week (**Sun** - **Sat**) and any applicable holiday ( **1** - **8**) in each of the applicable rows.

     b. Enter the start (**Active** is inclusive) and end (**Inactive** is exclusive) time in 24-hour clock format and avoid overlapping times.

     Example: A day shift from 08:00 - 19:59 and a night shift from 20:00 - 07:59.

     No conflict occurs when the actual start time is 08:00:*00* and the actual end time is 19:59:*59* for the day shift; and the actual start time is 20:00:*00* and the actual end time is 07:59:*59* for the night shift.

     For more examples, see *Adding Holidays* on page 379 and *Examples* on page 380.

> **Note:** For Mercury Security and ASSA ABLOY IP-enabled doors, the limit is 255 schedules. For Schlage IP/PoE mode doors, the limit is 16 intervals in all schedules combined. For SALTO doors, the limit is 1024 schedules.

c. Click to save the new schedule.

6. Select **Roles** > **Access Groups** and click **Add Access Group** to select the schedule and the doors.

   > **Note:** *SALTO doors only.* If a door is linked to a zone in the SALTO system, do not assign the access group a schedule that is less than five minutes in duration in the Active and Inactive fields.

   For more information, see *Adding an Access Group* on page 105.

7. Select **Roles** > **Roles** and select the role. Click the **Access Groups** tab and assign the access group to a role.

   For more information, see *Assigning an Access Group to a Role* on page 83.

## Editing Schedules

1. Select > **Schedules**.
2. Click the name of the schedule.
3. Edit the schedule as required.
4. Click to save your changes.

   > **Tip:** If a message indicates the Advanced Schedule option cannot be enabled when saving, do any of the following:
   >
   > - Save the schedule without Advanced Schedule selected. Some doors only support basic schedules.
   > - Find the access groups using the schedule and select another schedule.

## Deleting Schedules

> **Note:** When you delete a schedule that is currently used (such as by a door, panel or interlock), all references to the deleted schedule are replaced by the Never Active schedule.

1. Select > **Schedules**.
2. Click beside the schedule you want to delete.
3. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.

## Adding Holidays

1. Select > **Holidays**.
2. Click **Add Holiday**.
3. Enter a name for the holiday in **Name**.
4. Enter the specific date of the holiday.

   **Note:** For a recurring holiday, create a holiday for each future year.

5. If the holiday spans more than one day, fill out the **Additional Days** field.

   Default setting is **0** for a one-day holiday.

   Example: If 01/01/2020 is the date of the holiday and 2 additional days are specified, the holiday period is January 1, 2 and 3.
6. Select the number corresponding to the **Type** of holiday. (The holiday type number allows you to group specific types of holidays together.)

   **Note:** Up to 3 types of holiday groups are supported for SALTO doors.

7. Leave the **Preserve schedule days** checkbox unchecked so the holiday schedule will be active, rather than the regular schedule.

   If the **Preserve schedule days** checkbox is checked and it falls on the same day as a scheduled day, ACM will use the combined time frame of both the day of the week and the Holiday type.

   **Note:** If two holidays on the same date are added with different settings in this field (one is checked and the other is not checked), the settings of the last holiday added takes effect.

   **Note:** Not applicable for SALTO doors.

8. Click to save the new holiday.

## Editing Holidays

1. Select > **Holidays**.
2. Click the name of the holiday you want to edit.
3. Edit the information about the holiday as required.
4. Click to save your changes.

## Deleting Holidays

1. Select > **Holidays**.
2. On the Holiday list, click for the holiday you want to delete.
3. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.

## Examples

Noted below are two examples of setting up holidays and schedules.

### Example 1: Part-Day Holiday

All staff are attending an afternoon team function on December 18th, with work finishing at noon. On the 18th the doors need to unlock from 8 a.m. to noon, with access by Card Only mode after noon. The regular schedule for Monday to Friday is for the doors to open from 8 a.m. to 5 p.m.

1. Select > **Holidays**.
2. On the Holiday list, click to add a new holiday.
3. On the Holiday: Add page, enter:
   - **Name** (for example, `Company Half Day`).
   - **Date** (for example, `12/18/2020`).
   - **Type** (for example, `8`).
4. Click to save.
5. Select > **Schedules**.
6. Select the regular schedule on the Schedules list.
7. Click the **Advanced Schedule** checkbox to remove the default checkmark. The columns of holiday checkboxes are replaced by a single row of holiday checkboxes that supports a basic schedule.
8. On the first available free line (representing an interval in the schedule), enter `08:00` as the **Active** time and `11:59` as the **Inactive** time.
9. Click the checkbox for the **Type** selected in step 3 above (for example, **8**).
10. Click to save.

> **Tip:** To apply an advanced schedule that supports different holidays for intervals in a schedule, make sure the **Advanced Schedule** checkbox is selected. For example, if afternoon team functions

are held over two weeks on a Thursday and Friday (10th and 18th), add the two holidays (10th and 18th with **7** and **8** types, respectively) and then enter checkmarks for **Thu** and **7** in one row and **Fri** and **8** in another row. Save the schedule.

### Example 2: Additional Access Time

A special delivery is scheduled for December 20th, requiring additional access time from 8 p.m. to midnight. To create the additional access time without impacting the regular daily schedule, the Preserve schedule days option can be used. This option allows you to set separate access schedules for the same day.

1. Select > **Holidays**.
2. On the Holiday list, click to add a new holiday.
3. On the Holiday: Add page, enter:
   - **Name** (for example, `Late Night Access`).
   - **Date** (for example, `12/20/2020`).
   - **Type** (for example, `7`).
   - Click the **Preserve schedule days** checkbox.
4. Click to save.
5. Select > **Schedules**.
6. Select the regular schedule on the Schedules list.
7. Click the **Advanced Schedule** checkbox to remove the default checkmark. The columns of holiday checkboxes are replaced by a single row of holiday checkboxes that supports a basic schedule.
8. On the first available free line (representing an interval in the schedule), enter `20:00` as the **Active** time and `23:59` as the **Inactive** time.
9. Click in the checkbox for the **Type** selected in step 3 above (for example, **7**).
10. Click to save.

# Event Types

Event types are classifications of events that may occur during the operation of the ACM system. Event types are associated with specific event sources, such as doors, panels, and systems.

A number of event types are defined by default but you can add or delete event types as needed. The default events are listed below.

| Event Type | Source | Definition |
|---|---|---|
| **Communications** | Door<br>Panel<br>Subpanel | Events where two or more components cannot communicate with each other (for example, if a lock is offline with a hub, or if there is radio interference). Related events include:<br>• Lock offline with hub<br>• Panel offline<br>• Radio disturbance<br>• Subpanel communication disabled<br>• Subpanel offline<br>• Subpanel type mismatch<br>• VidProxy Image Service offline<br>• VidProxy Service offline |
| **Door held open** | Door | Covers door held events including:<br>• Door held masked<br>• Door held open<br>• Door held open pre-alarm<br>• Door held unmasked<br>• Extended door held disabled<br>• Extended door held enabled |
| **Forced Door** | Door | Covers forced door events including:<br>• Forced door<br>• Forced door masked<br>• Forced door unmasked |
| **Intrusion** | Intrusion Area, Maintenance, Panel, Point, System, User, Input, Intrusion SDI Device | Used for:<br>• Bosch intrusion events<br>• SDI intrusion device events<br>• General purpose input events from Mercury Security or VertX (general purpose inputs are inputs that are not used in a door). |
| **Intrusion DMP** | Intrusion Area, Panel, Zone, User | Used for DMP intrusion events. |
| **Invalid Credential** | Door | Relates to any door event where access is denied (e.g. Deactivated card attempt, Invalid card schedule, Access denied – occupancy level reached etc.). |

| Event Type | Source | Definition |
|---|---|---|
| **Maintenance** | Door<br>Panel<br>Subpanel | Primarily developed to cover events where action is required outside of the system (e.g. uploads, downloads, inconsistencies between panels etc.).<br><br>**Note:** There are other miscellaneous events which are also assigned to this event type. |
| **Output** | Outputs | Covers general purpose outputs - Mercury Security or VertX® outputs that aren't door strikes, including:<br>• Output point active<br>• Output point inactive<br>• Output point pulsed |
| **Power** | Door | Covers only low or critical battery events for doors. |
| **System** | System | Primarily used where the system is informing the user of an event. This includes global actions and linkages.<br><br>**Note:** This event type has also been used for other miscellaneous events (e.g. Card trace and Requests to enter for doors). |
| **System audit** | System/ Database<br>Credentials | Covers events where a record has been added, deleted or updated by the system. |
| **Tamper** | Door<br>Panel<br>Subpanel | Relates to all tamper events for panels or doors, including (but not limited to):<br>• Area disabled/enabled<br>• Lock jammed<br>• Occupancy count reached<br>• Panel transaction level reached |
| **User audit** | Door<br>Panel<br>Subpanel<br>Intrusion Panel<br>System/ Database | Where a user makes a change in the UI or in REST, including (but not limited to):<br>• APB requests<br>• Door-related requests<br>• Intrusion panel requests<br>• Records changed in database |
| | Credentials | Credential events, including (but not limited to):<br>• Biometric Enrollment Initiated when saving and enrolling ViRDI Biometrics tokens |

| Event Type | Source | Definition |
|---|---|---|
| **Valid Credential** | Doors | Access was granted to an identity that has access to the door and has swiped the card. For example, local grant, Opened unlocked door, Facility code grant, and more. |
| **Video** | Video | Video-related events, including:<br>• Connection Loss<br>• Motion Detected<br>• Video Loss |

**Note:** The Network and Offline lock event types are no longer in use and have been removed from the ACM system version 5.10.0 onwards.

## Adding Event Types

1. Select > **Event Types**.
2. Click **Add Event Type**.
3. Enter a name for the new event type.
4. Select the **Alarm** checkbox to generate an alarm for the event type.
5. Complete the remainder of the page with the required settings.
6. Click **Save**.

## Editing Event Types

1. Select > **Event Types**.
   The Event Types list is displayed.
2. From the Event Types list, click the name of an event type.
3. On the Event Type Edit page, make any changes that are required.
4. Click to save your changes.

## Deleting Event Types

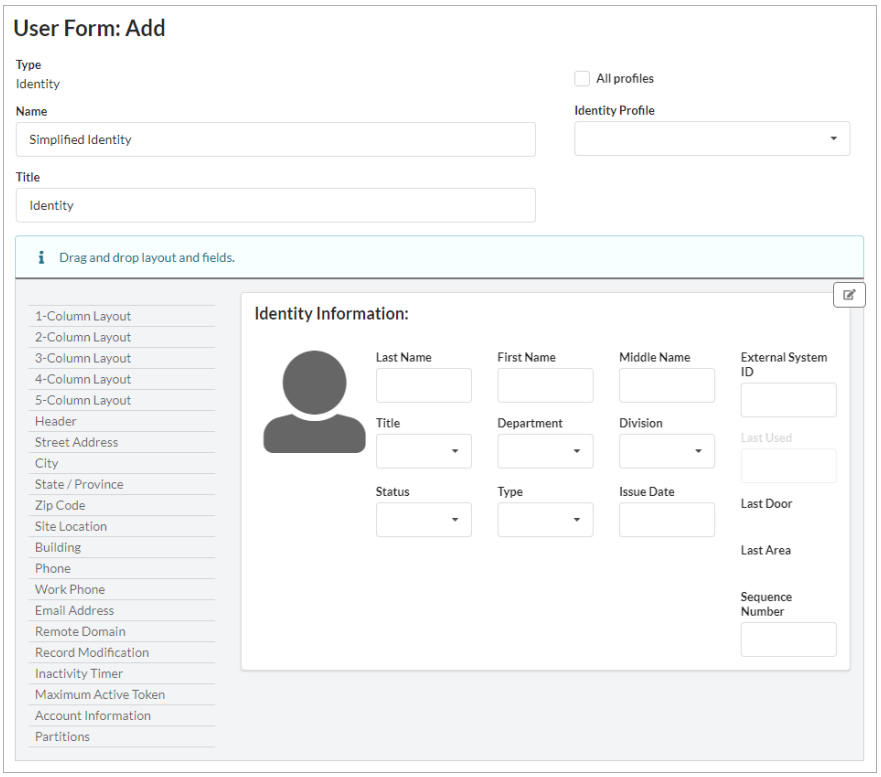
**Note:** System default event types cannot be deleted. You can only delete event types that have been manually added to the system.

1. Select > **Event Types**.
2. Click beside the event type you want to delete.
3. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.

# User Forms Overview

ACM Super Admin users only

User forms provide a drag-and-drop interface for identity management. For example:




Customize the identity and tokens tabs or create additional ones, and then assign them to ACM operators. For more information, see:

- *Adding and Customizing Tabs with User Forms* below
- *Assigning Tabs to Identities with User Forms* on the next page
- *Editing User Forms* on page 387
- *Deleting User Forms* on page 387

## Adding and Customizing Tabs with User Forms

Choose User Forms to customize the Identity and Tokens tabs, and add any number of custom tabs, inserted in alphabetical order, after the built-in tabs on the Identities page.

Before you begin, add any new user-defined fields. For more information, see *Adding and Assigning Tabs to Identities with User Fields* on page 388.

1. Select ⚙ > **User Forms**.

   The built-in identity and token forms are visible on all identities by default (★) and cannot be edited and deleted.
2. Click **Add User Form**.

3. Select a form type for customization:
    - **Identity** — A form with pre-populated fields, which can be displayed instead of the default Identity tab.
    - **Token** — A form with pre-populated fields, which can be displayed instead of the default Tokens tab.
    - **Custom** — A blank form, which can be displayed as an additional tab that is customized to meet your requirements.
4. Click **Next** and optionally assign the form to one or more identity profiles. Enter:
    - **Name** — A name for the form.
    - **Title** — A label for the tab on the identity page.
    - **All Profiles** checkbox — All identity profiles, current and future, to be assigned to the form.
    - **Identity Profile** — If All Profiles is not selected, select one or more identity profiles.
5. To customize the form, do any of the following:
    - Drag and drop a layout from the list of layouts. This is required for a blank custom form and optional for a pre-populated form.
    - Drag and drop **Header** to enter a label for the items.
    - Drag and drop a field from the list of built-in and user-defined fields.
        - **Last Name** and **Status** are required for an identity record.
    - Click the **Advanced Edit** icon in the upper-right corner.
        - To make a field read-only which means it is grayed out and not editable by the operator, click it and select **Properties**. Click the **Read-only** checkbox and click **Save**.
        - To delete a field, hover your mouse over it and select **Remove**.
        - To delete a layout and its items, hover your mouse over it and click on the bottom edge.
6. Click **Save** to save the new form.

After you add a new form, see *Assigning Tabs to Identities with User Forms* below.

## Assigning Tabs to Identities with User Forms

After one or more identity or token forms are created, display them to all ACM operator identities or only specific identities.

After one or more custom forms are created, display them to all ACM operator identities or only specific identities.

> **Note:** Delegations can restrict operators from editing and viewing the list of assignments.

On the User Forms list, do any of the following:

- For an identity or token form:
    - To display an identity or token form, click the ☆ default icon next to the form to make it the default. The default icon changes to ★.

      The identity or token tab will be displayed to all operator identities. To reverse this change, click ★.

- For a custom form:
  - To display one or more custom forms to all identities, click the public icon next to each custom form. The public icon changes to .

    The custom tab will be displayed to all operator identities. To reverse this change, click .
- For any form type:
  - To define the operator identities who can view the form, click **Assign** and select the identities. Click to move them from the **Available** list to the **Members** list. To reverse these changes, click to move them back to the **Available** list. Click **Save**.

    The identity, token or custom tab will not be displayed to all operator identities. Only the selected operator identities can view it.

## Editing User Forms

To edit an identity, token or custom form:

1. On the User Forms list, click the name of the form.
2. Do any of the following:
   - Add, edit or delete fields.
   - Add, edit or delete a layout.
3. Click **Save**.

## Deleting User Forms

You can delete an identity, token or custom form that is not set to default or not assigned to any identities. In addition, the built-in forms cannot be deleted.

1. Select **>User Forms**.
2. Click next to the name of the form. The button is not displayed if any identities are assigned to the form.
3. When the confirmation message is displayed, click **OK**.

# User Defined Fields

User defined fields are custom fields that you can add to the Identities page to capture organization specific information for each identity.

To add user defined fields to the Identities page, you must also add a user defined tab to host the fields.

Information captured by user defined fields can be used on badges to display important details about each identity.

User defined fields can also be used for advanced searching for identities. For more information, see *Searching for an Identity* on page 64.

## Adding a Field for User Forms, Tabs and Lists

User-defined fields are used to collect additional details about users on the Identities screen. After you add all the fields, add at least one tab to display the new fields. For more information, see *Adding and*

*Customizing Tabs with User Forms* on page 385 and *Adding and Assigning Tabs to Identities with User Fields* below.

1. Select >**User Fields**.
2. Click **Add User Defined Field**.
3. Enter a name for the new field in the **Name** field.
4. Select the field **Type**:
   - **String** — The field supports words and numbers.
   - **Integer** — The field supports numbers only.
   - **Boolean** — The field is a checkbox that works like a Yes or No question. Check the box to indicate 'yes' and clear the box to indicate 'no.
   - **Date** — The field supports a date only. Click the field to display a calendar and select a date.
5. Click to save the new field.

> **Note:** User-defined fields cannot be edited, only deleted.

## Adding and Assigning Tabs to Identities with User Fields

You must add a new tab to host user-defined fields before using them on the Identities page. Add tabs after you've added all the fields that you need.

> **Tip:** It is recommended to add a tab and user-defined fields on the Identities page using identity, tokens and custom forms in a drag-and-drop interface. For more information, see *Adding and Customizing Tabs with User Forms* on page 385.

1. Select > **User Fields**.
2. Click the **Tabs** tab.
3. Click **Add User Defined Tab**.
4. Enter a name for the new tab in **Name** and click .
5. From the **Available** list, select all the user-defined fields that should be displayed on the tab and click to add them to the **Members** list.

   To remove a field from the tab, select the field from the Members list and click .
6. Click to save your changes.

## Adding User Defined Fields to Tabs

1. Select > **User Fields**.

   The User Fields list is displayed.
2. From the User Fields list, click the **Tabs** tab.
3. Click the name of the tab that you want to edit.
4. Edit the tab details as required.
5. Click to save your changes.

## User Defined Fields - Deleting Fields

**NOTE**: You cannot delete user defined fields if they are used in a tab. To delete a field, you must remove it from all tabs first.

1. Select > **User Fields**.
2. If the symbol displays for the field you want to delete:
   a. Click to delete the field.
   b. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.
3. If the symbol does not display for the field you want to delete, this is because the field is currently used by a tab. To remove a field from a tab:
   a. Select the **Tabs** tab then click the name of the tab that the field appears in.
   b. On the following page, select the field from the Members list then click .

      The field is removed from the tab and returned to the Members list.
   c. Click .

## User Defined Tabs - Deleting

User defined tabs can be deleted as required. However, you cannot delete user defined fields if they are used in a tab.

1. Select > **User Fields**.
2. Select the **Tabs** tab.
3. Click for the tab you want to delete.
4. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.

# User Lists

Many fields on the Identity page involve selecting a value from a drop down list. While there are several default values for these fields, you can add more options using the User Lists feature.

For example, if you want to add departments that are specific to your organization, you would use this feature to add those options to the Departments drop down list.

## Adding Items to a List

**Note:** Any changes you make to the lists are automatically included in identity-related collaborations.

1. Select > **User Lists**.
2. Click the name of the list you want to add items to.
3. On the User List Edit screen, enter a new list option in the **New Value** field and click .
4. Repeat the previous step until all the new values you want are listed in Current Values.
5. Click to save your changes.

## User Lists - Editing Items

Any changes you make to the lists are automatically included in identity related collaborations.

1. Select > **User Lists**.
   The User Defined Lists list is displayed.
2. On the User Defined Lists list, click the name of the list you want to edit.
3. To add a new option, enter the new option in the **New Value** field then click .
   The new value is added to the Current Values list.
4. To delete a value, select the option from the Current Values list and click .
5. Click to save your changes.

## User Lists - Deleting Items

1. Select > **User Lists**.
   The User Defined Lists list is displayed.
2. On the User Defined Lists list, click the name of the list you want to edit.
3. Select the option you want to delete from the Current Values list then click .
4. Click to save your changes.

The option you deleted is no longer listed on the Identities page.

# System Settings

Use > **System Settings** to:

- Customize default values for system-wide settings in the ACM system configure. For more information, see *System Settings - General Fields* on page 394.
- Configure remote authentication of ACM users with an external domain server. For more information, see *Remote Authentication - Introduction* below.
- Identify the external domain servers used for remote authentication. For more information see *System Settings - External Domains list* on page 399.

## Remote Authentication - Introduction

With remote authentication, ACM Client users can use their local domain username and passwords to access the ACM system. Remote authentication uses an external domain server to authenticate users that need access to the system, or to secure an LDAP Identity pull collaboration type. A separate password configured in the ACM appliance is not needed. However, user access permissions are still based on the roles they are assigned within the ACM appliance.

Before remote authentication can be configured on the ACM appliance, a system administrator with privileges on all the servers required to support remote authentication needs to:

- Add one or more external domains
- Add one or more AD or LDAP servers to each domain to the system
- Issue root certificates for each domain
- Enable each remote host to present its SSL certificate on connection to the ACM server software

Configuration of the external domain servers and the creation of their root certificates is outside the scope of this document.

To allow remote authentication, you must:

1. Connect to the external domain servers hosting the AD or LDAP servers you want used for authentication and validate the SSL certificates they present. *System Settings - External Domains list* on page 399.
2. Specify the default domain and server that hosts the AD database to use for authenticating ACM software users, and enforce certificate authentication. For more information see *System Settings - Remote Authentication page* on page 397.

Secure Socket Layer (SSL) certificates are used to verify the remote hosts and to encrypt all the log in traffic between connected hosts. Only ACM system operators with administrative privilege and the following delegations assigned to their role can validate SSL certificates:

- External Domains Validate Certificates—delegation required to validate an SSL certificate from a Windows AD host
- Collaboration Validate Certificates—delegation required to validate an SSL certificate from an LDAP database host in a Collaboration using the Identity Pull LDAP server collaboration type

You can set up different identities to be authenticated by different domains. Each identity must be configured to use one of these domains for authentication. This is done in the Account Information: section on either the Identity: Add or Identity: Edit panel of the given Identity. For more information, see

## Configuring Remote Authentication Using SSL Certificates

Remote or external domains only. For Super Admin users with the External Domains Create Certificate, External Domains Destroy Certificate, External Domains List Certificates, External Domains Load Certificate and External Domains Validate Certificates delegations assigned to their role.

Certificates can be recognized by the ACM appliance in two ways:

- Pinned SSL certificates—Certificates from remote hosts in external domains that are accepted manually by an ACM system administrator so that the remote host can connect automatically. These certificates are trusted as long as they are not revoked manually by an ACM system administrator.
- Trusted SSL certificates—Certificates from remote hosts in external domains that are imported into the ACM server software so that the remote host can connect automatically. They are valid until the certificate expires.

**Note:** To provide maximum security strength for your ACM system, ensure the certificate meets the U.S. government's National Institute of Standards and Technology (NIST) Special Publication 800-131A (SP 800-131A) standard.

If your ACM appliance to ACC integration deployment is having trouble connecting, review the certificate requirements for the two systems. You may need to update the certificate on the ACM appliance to resolve the connection issues between the two systems.

## About Certificate Pinning

When SSL certificates from a server in an external domain have not been exported from that server and uploaded to the ACM server they cannot be automatically trusted.

However, a remote server can present its SSL certificate to the ACM server so that an administrator can choose to trust it based on the administrator's certainty that the certificate is valid. In the ACM server, after an SSL certificate is accepted manually, it will be trusted as long as the unique fingerprint embedded in the certificate presented by the remote server each time it is connected to the ACM software is the same as the certificate originally accepted by the ACM system administrator. A certificate that is trusted in this way is known as a pinned certificate.

Pinning a certificate allows you to trust a certificate that has not been uploaded from a remote server, however the responsibility for ensuring that the certificate can be trusted is assumed by the ACM system administrator who pins the certificate. To ensure that an SSL certificate is valid before it is pinned, the ACM system administrator should compare the SSL certificate at the remote host to the certificate received from the remote host to confirm the SHA-256 fingerprints are identical.

## Requirements for Using Pinned Certificates

On the remote Windows server (for example, an Active Directory (AD) server, if you are enabling remote authentication using the AD of your company), the following tasks must be completed:

1. Configure a Windows domain controller. For an LDAP collaboration, TLS encryption must be activated.
2. Obtain the fully-qualified domain name of the DNS server for remote server's domain.
3. Enable AD Certificate Services.
4. Create a root certificate and a Domain Controller Authentication certificate.

These tasks are outside the scope of this document.

## Requirements for Using Trusted Certificates

On the remote Windows server (for example, an Active Directory (AD) server, if you are enabling remote authentication using the AD of your company), the following tasks must be completed:

1. Configure a Windows domain controller. For an LDAP collaboration, TLS encryption must be activated.
2. Obtain the fully-qualified domain name of the DNS server for remote server's domain.
3. Enable AD Certificate Services.
4. Create a root certificate and a Domain Controller Authentication certificate.
5. Export the Domain Controller's root CA certificate in Base-64 encoded X.509 (.CER) format. (Do not export the private key.)

   **Important:** Use OpenSSL to convert the file from `.cer` format to `.pem` format before you upload the file to the appliance.

6. Upload the certificate to the ACM appliance. For more information, see *Certificate Upload page* on page 402.

These tasks are outside the scope of this document.

## Pinning or Trusting Certificates in the ACM System

Once you have all the requirements for either pinning or trusting the certificate for an external server, log in to the ACM Client, and complete the following steps:

1. In the top-right, select >**System Settings**.
2. Select the **External Domains** tab.
3. Click **Add External Domain**.
4. On the External Domain: Add New page, enter a name for this external domain.
5. In the **Server** field, enter the full DNS name of your domain controller.
6. Click to display the trust level of this domain. The default setting is "Untrusted".
7. Click Validate Certificate.
8. Click . The domain controller is added to the Current Servers list.
9. Select the **Remote Authentication** tab.

   **Note:** The Default Domain and Default Server options are not required for remote authentication.

10. Select the **Validate Certificate** checkbox.
11. Click .
12. Repeat the previous steps on each ACM appliance in your system that requires remote authentication.

13. Enable remote authentication for each identity that will be logging into the ACM appliance:
    a. Open the Identity:Edit page for a user who will be using remote authentication.
    b. Under the Identity tab, select the **Remote Authentication?** checkbox in the Account Information area.

    > **Note:** Do not enable MFA for the ACC user account.

    c. In the **Login** field, enter the user's ACM system login name.
    d. In the **Remote Domain** drop down list, select the external domain that you added earlier.
    e. In the **Remote Login** field, enter the user's Active Directory domain identity. Enter the login name in this format: *username@domain.org*.

       For example: j.smith@motorolasolutions.com

    f. Click .

### Enabling Remote Authentication for ACM Client Users

Enable remote authentication for each identity with permission to log into the ACM Client:

a. Open the Identity:Edit page for a user who will be using remote authentication.
b. Under the Identity tab, select the **Remote Authentication?** checkbox in the Account Information area.

> **Note:** Do not enable MFA for the ACC user account.

c. In the **Login** field, enter the user's ACM system login name.
d. In the **Remote Domain** drop down list, select the external domain that you added earlier.
e. In the **Remote Login** field, enter the user's Active Directory domain identity. Enter the login name in this format: *username@domain.org*.

   For example: j.smith@motorolasolutions.com

f. Click .

Now, when this user logs in to the ACM Client, they use their network login name and the password.

## System Settings - General Fields

Set ACM system-wide settings on the **General** tab in > **System Settings**:

> **Note:** Certain user settings in > My Account will override the general settings.

| | |
|---|---|
| **Enhanced Access Level** | Indicate that this system will use enhanced access levels for Mercury Security panels. Enhanced access levels allow Mercury Security panels to accept more access groups per token. |

| | |
|---|---|
| **Allow Duplicate PINs** | Duplicate PINs is an option available for an organization that wants to allow badge holders to have non-unique PINs. This option cannot be used with the PIN Only and Card or PIN door modes as it does not allow tracking of an individual badge holder.<br><br>After you enable duplicate PINs, the available Door Mode options are:<br><br>• **Card Only** — This door can be accessed using a card. No PIN is required.<br>• **Card and Pin** — This door can only be accessed using both a card and a PIN.<br>• **Facility Code Only** — This door can be accessed using a facility code.<br><br>**WARNING —** After duplicate PINs are allowed, this cannot be reversed, and you cannot use PIN Only and Card or PIN door modes. Only enable this option if you have a specific requirement for duplicate PINs.<br><br>Do the following before allowing duplicate PINs to ensure that no doors are in either PIN Only or Card or PIN door modes:<br><br>1. Select **Physical Access** > **Doors** to navigate to the Door list.<br>2. For each door currently in either PIN only, or Card or PIN mode:<br>  • Select the checkbox beside the door.<br>  • Either select **Door Action** > **Restore** to restore to the configured door mode or select an alternative mode from the Door Mode dropdown list.<br><br>To allow duplicate PINs, check this box then:<br><br>• Click **OK** when the message 'Enabling duplicate PINs is an irreversible setting and cannot be undone. Are you sure you want to continue?' displays.<br>• Click **OK** when the message 'Proceed with enabling duplicate PINs?' displays.<br><br>**Note:** The system will check Door Policies, Global Actions, Scheduled Jobs, Panel Macros, and Interlocks to ensure there is no conflict with duplicate PINS (e.g. doors are in PIN Only mode). If there are any conflicts these will have to be corrected before allowing duplicate PINs. If there have been any previously defined linkages, triggers or interlocks that are based on PIN Only or Card or PIN event types, they will fail to execute. |
| **Badge Template Photo Height** | A new value in pixels to change the default height for displaying the ID photo used for badge templates on the screen then click .<br><br>The default value of 153 px is approximately 1½ inches or 3.5 centimeters. |
| **Badge Template Photo Width** | A value in pixels to change the default width for displaying the ID photo used for badge templates on the screen then click .<br><br>The default value of 117 px is approximately 1 inch or 2.5 centimeters. |

| | |
|---|---|
| **Force Password Change** | For all users with the Force Password Change delegation assigned to their role.<br><br>A checkbox to force the identity to change the password at the next login to the ACM system. After the password is changed by the identity, the checkbox is deselected automatically.<br><br>This option is enabled by default.<br><br>**Note:** The system will only apply this setting to new identities.<br><br>**Tip:** To apply the Force Password Change operation to a group of identities, see *Performing an Identity Batch Update* on page 101. See *Searching for an Identity* on page 64 to specify Force Password Change in the Search Field. |
| **Identity Auto Increment Field** | Enable the system to automatically increments the read-only Sequence Number field on the Identity page.<br><br>This option is disabled by default.<br><br>**Note:** The system will only apply this setting to new identities. |
| **Identity Auto Increment Start** | If you enabled Identity Auto Increment, enter the number the system will start counting from then click .<br><br>The default value is 1.<br><br>**Note:** The system will only apply this setting to new identities. |
| **Identity Auto Increment Step** | If you enabled Identity Auto Increment, enter the value the system uses to increment the sequence number then click .<br><br>For example, if you leave the default value of 1, the identity Sequence Number will count 1, 2, 3 (etc.). If you enter 2, the identity Sequence Number will count 1, 3, 5 (etc.).<br><br>**Note:** The system will only apply this setting to new identities. |

| | |
|---|---|
| **Language** | A language that the system will display by default.<br><br>Each user with access to the ACM system will be able to set their own language preferences from the My Account page. For more information, see *Setting Your Preferred Language* on page 455.<br><br>Click **Translate Default Data** to translate all of the system default values into the selected language. It is recommended that you only perform this action once, or your reports and logs will display values in multiple languages. |
| **Maximum Active Tokens** | The maximum number of tokens that can be active per identity then click . |
| **Maximum Login Attempts** | The maximum number of attempts a user has to log into the ACM system before they are locked out, then click .<br><br>The user is locked out of the ACM system for 10 minutes and further login attempts will result in the lockout time increasing. Authorized operators can reset the password to bypass the lockout.<br><br>The default value is 5. |
| **Password Strength Enforced** | Enable a minimum password strength requirement for ACM system upgrades which can be performed using any user account. The password must contain 8 to 40 characters, and at least 1 uppercase letter, 1 lowercase letter and 1 digit. For more information, see *Logging In* on page 21. |
| **Post Roll** | The number of seconds a camera continues to record after a recorded video event. |
| **Pre Roll** | The number of seconds of video that is automatically added before a recorded video event. |
| **Private Message** | A short message to display on the login screen. |
| **Show Identity Photos** | Enable a photo to be displayed beside each identity reference. |
| **System Message** | A title you want to use for the system then click .<br><br>The title is displayed under the Access Control Manager banner on each screen, and the title is used for all messages sent by the system. |
| **System Support** | The contact details of your Avigilon support representative then click .<br><br>This information is displayed when a user clicks **Support**. |
| **Token Expiration Time** | The default number of days before a token expires then click . |
| **Use/Lose Threshold** | The default number of days a token can be unused before it is automatically deactivated, and then click . |
| **Video Windows Count** | The maximum number of video display windows that can be open at the same time, then click . |
| **Create Report** | Generate a PDF of the values on this page. |

## System Settings - Remote Authentication page

When you select the **Remote Authentication** tab on the System Settings screen, the Remote Authentication panel is displayed.

On this panel, define the default domain and server that hosts the Active Directory database used to authenticate network users. This enables secure connections and encrypted traffic between the AD server and the ACM servers and its clients. ACM Client users can then use their local domain username and passwords to access the ACM system.

| Feature | Description |
|---|---|
| **Default Domain** | Select a domain from the drop down list.<br><br>Only the external domains that have been added to the system are listed. |
| **Default Server** | Enter the name of the default server in the selected domain. |
| **Validate Certificate** | Check this box to enable the system to validate certificates from remote servers before use.<br><br>The default setting is not checked. Use the default setting only if you do not need to validate certificates from remote servers.<br><br>**CAUTION —** Risk of security breaches. When certificate validation is not enabled, certificates are ignored by the ACM server software. Traffic between the ACM appliance and external domains is unencrypted and can be easily compromised. To ensure secure connections and encryption of all traffic, enable the Validate Certificate option on the Remote Authentication tab of System Settings. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |
| **Create New Report** | Click this button to generate a PDF of the values on this page. |

# Re-trust Certificates

After upgrading to ACM 6.50 or later, you must re-trust your SSL certificates for external domains and identity LDAP pull collaborations before users authenticated by those mechanisms can access ACM. Only systems with uploaded certificates have trust maintained after the upgrade. This does not apply to implementations that do not use SSL certificates or do not have external domains or identity LDAP pull collaborations.

When you first Log In after an upgrade, a banner with the following warning appears on each page:

> **WARNING —** Remote identity authentication and identity LDAP pull collaboration will not work until SSL certificates are re-trusted.

**Note:** If you upload a certificate after trusting it, the trust needs to be removed or reapplied.

**Note:** It is recommended that you remove any untrusted certificate records.

## Re-trust certificates for external domains

To re-trust certificates for external domains:

1. In the top-right, select >**System Settings**.
2. Openthe**ExternalDomains**tab.
   The certificates are color-coded:

   - Green means the certificates are trusted.
   - Yellow means the certificates are pinned.
   - Red means the certificates are untrusted.
3. For each red (untrusted) certificate, click **Validate Certificate**.
4. Check the **Trust** box.
5. Click **Save**.

### Re-trust certificates for identity LDAP pull collaborations

To re-trust certificates for Identity LDAP pull collaborations:

1. In the top-right, select >**Collaboration**.
2. SelecttheIdentityLDAPpullcollaborationfromthelist.
   The certificates are color-coded:

   - Green means the certificates are trusted.
   - Yellow means the certificates are pinned.
   - Red means the certificates are untrusted.
3. Check the **SSL Validate Certificate** box.
4. Check the **Trust**box.
5. Click **Save**.

### Dismiss the warning banner

To dismiss the warning banner:

1. Open the **Remote Authentication** tab.
2. Check the **Dismiss Warning Banner** box.
3. Click **Save** .

Clicking **Save** will dismiss the warning banner for all users and cannot be undone. Before you dismiss the warning banner, re-trust all certificates used for external domains and identity LDAP pull collaborations.

## System Settings - External Domains  list

When you select the **External Domains** tab from the System Settings page, the External Domains  list is displayed. This page lists any external domains that have been added to the system.

An external domain must be added before you can use remote authentication. For example, to connect the ACM system to use your company's Active Directory (AD) to authenticate users, you must add the company domain server to the External Domains Listing.

**Important:** After upgrading to ACM 6.50 or later, you must re-trust your SSL certificates for external

domains and LDAP pull collaborations before users authenticated by those mechanisms can access ACM. For more information, see *Re-trust Certificates* on page 398.

You can grant remote authentication access to individual badge holders from the Identity page. For more information, see *Identities* on page 60.

| Feature | Description |
|---|---|
| **Name** | The name of this external domain.<br><br>Click the name to edit the external domain. For more information, see *System Settings - External Domain: Edit page* on the next page. |
| **Delete** | Click to delete the selected external domain. |
| **Add External Domain** | Click this button to define a new external domain. For more information, see *System Settings - External Domains Add page* below. |
| **Create New Report** | Click this button to generate a PDF report of the listed domains. |
| **Certificates** | Click this button to access the Certificate list.<br><br>From this page you can upload one or more certificates to give remote browsers access to the ACM system.<br><br>Uploaded certificates persist after upgrading to ACM 6.50 or later and do not require re-trusting. |

## System Settings - External Domains Add page

When you click **Add External Domain** from the External Domains list, the External Domain: Add New page is displayed.

You must add an external domain to connect to a remote server for user validation using your company's Active Directory (AD), or using LDAP.

Before you validate the certificate presented by the remote server in the external domain, it is recommended that you find out the value of the SHA-256 fingerprint of the remote server's certificate. Then you can compare that value to the one in the certificate displayed in the ACM software.

| Feature | Description |
|---|---|
| **External Domain** | Enter the name of this external domain. Never append the extension `.lan` or `.local` |
| **New Server** | Enter the full-qualified domain name (FQDN) of the server in the external domain and then click.<br><br>You can enter the IP address of the server, although this is not recommended as it is more likely to change than the FQDN. |
| | Display the current trust level of this domain. The default setting is "Untrusted". |

| Feature | Description |
|---|---|
| **Validate Certificate** | Click to validate the certificate presented by the server. If the certificate from the remote server is:<br>• Fully trusted—A "Certificate Verified" message is displayed. Click **OK**. The certificate status is updated to Trusted.<br>• Untrusted—The certificate is displayed. Compare the SHA-256 fingerprint to the actual certificate defined. If they match, click **Trust** and the certificate status is updated to Pinned. Otherwise click **Deny** to update the certificate status to Untrusted, or **Cancel** to close the dialog box without making any changes.<br>• Not available—An error message is displayed, and the certificate status remains Untrusted. |
| | Hide the current trust level of this domain. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

## System Settings - External Domain: Edit page

When you click the name of a domain from the External Domains  list, the External Domains: Edit page is displayed.

Make any changes that are required.

| Feature | Description |
|---|---|
| **External Domain** | Enter the name of this external domain. Never append the extension `.lan` or `.local` |
| **New Server** | Enter the full-qualified domain name (FQDN) of the server in the external domain and then click.<br>You can enter the IP address of the server, although this is not recommended as it is more likely to change than the FQDN. |
| | Display the current trust level of this domain. The default setting is "Untrusted". |
| **Validate Certificate** | Click to validate the certificate presented by the server. If the certificate from the remote server is:<br>• Fully trusted—A "Certificate Verified" message is displayed. Click **OK**. The certificate status is updated to Trusted.<br>• Untrusted—The certificate is displayed. Compare the SHA-256 fingerprint to the actual certificate defined. If they match, click **Trust** and the certificate status is updated to Pinned. Otherwise click **Deny** to update the certificate status to Untrusted, or **Cancel** to close the dialog box without making any changes.<br>• Not available—An error message is displayed, and the certificate status remains Untrusted. |
| | Hide the current trust level of this domain. |
| | Click this button to save your changes. |

| Feature | Description |
|---|---|
| | Click this button to discard your changes. |

## System Settings - Certificates list

When you click **Certificates** from the External Domains list, the Certificates list is displayed.

Certificates that have been uploaded to the system are listed on this page. Certificates are used by browsers to confirm that systems are safe for users to access.

| Feature | Description |
|---|---|
| **Name** | The name of the certificate file. |
| **Size** | The size of the certificate file. |
| **Upload Date** | The date the file was uploaded. |
| | Click this button to delete the certificate.<br>Deleting a certificate will cause the appliance to reboot. |
| **Add New Certificates Listing** | Click this button to upload a new certificate for this external domain.<br>**Note:** To provide maximum security strength for your ACM system, ensure the certificate meets the U.S. government's National Institute of Standards and Technology (NIST) Special Publication 800-131A (SP 800-131A) standard.<br>If your ACM appliance to ACC integration deployment is having trouble connecting, review the certificate requirements for the two systems. You may need to update the certificate on the ACM appliance to resolve the connection issues between the two systems. |

## Certificate Upload page

Use this page to upload an external domain server certificate in `.pem` format to the ACM application. This allows ACM Client users to log in using their network user ID and password through a fully trusted Active Directory (AD) server on an external domain.

> **Tip:** The exported certificate must be converted from `.cer` format to `.pem` format by a system administrator on the AD server before it is uploaded to the ACM server.

There must be a certificate for every server that has been added to the system as part of the external domain.

| Feature | Description |
|---|---|
| **Upload Certificate file:** | Click **Browse** to locate and select the certificate in the Choose File to Upload dialog box. |
| | Click this button to save your changes. |
| | Click this button to discard your changes. |

# Badge Templates and the Badge Designer

This feature requires a license. Contact your Avigilon support representative for more information.

Badge templates define the layout of badges or cards that are used to access doors within your access control system. They are created by a qualified operator using the Badge Designer. Multiple badge templates can be defined in the ACM system.

Select > **Badge Designer** to access the Badge Templates page. From this page, you can add a new badge template, or select a badge template to edit, with the Badge Designer.

The Badge Designer is used to design the appearance and content on a badge template. You can add photos, logos, text, and database fields to a badge template and position these elements on the layout. A badge template can specify colors and fonts depending on the values provided.

For example, if an employee is specified as part-time, the color used for the employee's name can be changed from black to orange, making it easier for guards to differentiate between full-time and part-time employees. You can differentiate identities with different access privileges, such as access to certain buildings on a campus, or specific floors in a multi-tenant office building, using graphics such as company logos and insignias, or text.

A badge template is used when a badge is generated for a badge-holder to both format the badge and populate it with data from the Identities database. At least one badge template to assign to identities must be created before badges can be printed using **Identities** > **Badge**. Badges are usually printed when a person who requires a badge is enrolled into the ACM system using the Identities feature. When printing the badge, an enrollment officer or administrator specifies a badge template and then generates (prints) a badge. The badge has all relevant information automatically placed on the badge.

**Note:** Badge templates can be designed as either one- or two-sided. A two-sided badge must be printed by a badge printer possessing duplex capability.

## Using the Badge Designer

Use the Badge Designer to create templates that define the layout and appearance of access badges.

A badge template defines the basic attributes of a badge that are used when a new badge is generated for an identity: size and background color, plus a variety of dynamic and static fields and images. Dynamic fields and images pull the unique information about the badge holder from the Identities database for each individual badge and static objects are the text strings and graphics printed on every badge. For each object, you can specify its location and appearance.

| | Field | Image |
|---|---|---|
| **Dynamic** | **DBField**: A data field object specifies the information about the identity that you want on the badge, such as first and last name, ID number, title, position, rank and so on. | **Picture:**: A picture object specifies the size and location of the photo of the identity on a badge.<br><br>The actual photo used for an identity when a badge is generated is a photo saved in the Identities database that was either captured with a badge camera, or uploaded, and saved. |

| | | |
|---|---|---|
| **Static** | **Text**: A text object specifies the text that appears on every badge generated with this template. | **Graphic**: A graphic object specifies the name of an uploaded graphic file image file that appears on every badge generated with this template. |

You must create at least one badge template before you can print a badge at **Identities** > **Badge**. Depending on the requirements of your site, you may need one or more badge templates.

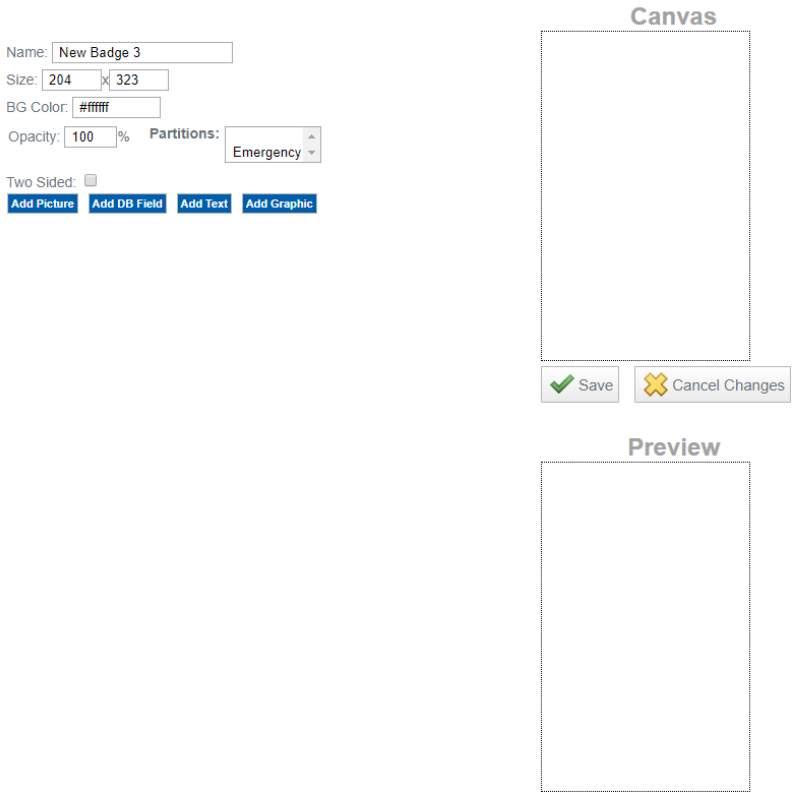
> **Note:** Badge templates can be designed as either one- or two-sided. A two-sided badge must be printed by a badge printer possessing duplex (double-sided printing) capability.

### Opening the Badge Designer

Select > **Badge Designer** to open the Badge Templates page. From this page, click **Add Badge Template** or the name of an existing badge template to open the Badge Designer page.

### Formatting the Appearance of a Badge Template

Use the canvas data fields that appear at the top of the Badge Designer page to set the size, color, and other format details. Next to the canvas data fields is the canvas area, with the preview area beneath that show the changes to the template as you make them.




All measurements in the Badge Designer are in pixels, at a resolution of 100 pixels per inch, equivalent to 40 pixels per centimeter.

1. Give the badge template a name, or change it.
2. Change the size of the badge if needed. Values are entered in pixels. The default size is equivalent to a print area of 2 x 3.25 inches, or 5 x 7 centimeters.
3. Click in the **BG Color** field to open the color picker. Enter a hex code or select a color for the background.
4. Click **OK** to close the color picker, then click to apply the background color to the canvas and the preview.
5. Change the value in the **Opacity** field only if you want the background color to be semi-transparent or transparent. For example if you are overprinting badge information on a preprinted badge. Click to apply the opacity to the preview.

**Create a Two-Sided Badge Template**

1. Select the **Two Sided** checkbox.

   The Back Side button appears at the top of the page.
2. **Important:** Click to save this setting.

   To view the back of the badge, at the top of the page, click **Back Side**. To view the front of the badge, at the top of the page, click **Front Side**.

**Adding and Editing Objects**

You can add four types of objects to a badge template to define the information that appears on the identity badges generated by this template:

| Object | Definition |
|---|---|
| **Picture** | Dynamic. A photo of the identity supplied by the Identities database. You can have only one photo per side of a badge. |
| **Data Field** | Dynamic. An item of information supplied by the Identities database, such as the person's name. You can have many data fields per side of a badge. |
| **Text** | Static. Text such as a company name, or slogan to appear on every badge. You can have many data fields per side of a badge. |
| **Graphic** | Static. Image files such as a logo, insignia or texture, to appear on the badge, uploaded into the template. You can have many images per side of a badge. |

When you add an object, additional fields for that object appear below, and an appropriate placeholder appears on the Canvas. You can expand and collapse each object in the list to access its field settings.

1. On the canvas you can position any object by clicking and dragging with the mouse.
2. Select the object in the list to edit its settings.
3. Any change you make to the object's field settings are reflected on the canvas.
4. Click beside an object to delete it from the list. Objects deleted from the list are not deleted from the canvas until you save changes.

5. Click ✔ frequently to save changes and show the result in the Preview.

> **Tip:** Add objects to the Canvas from largest to smallest in size. The Canvas displays objects in the order they are added not by the Layer Order setting, so large objects can obscure smaller ones. Save the template to refresh the Preview and see the actual result.

**Adding and Editing a Picture Object**

1. Click the **Add Picture** button to add a photo object to the canvas.
2. Click **Photo** to hide or show the photo object settings.
3. Adjust the appearance of the photo.

> **Tip:** The default dimensions of the photo on the badge displayed on the screen are defined by the values set on the **System Settings** page for **Badge Template Photo Height** and **Badge Template Photo Width** and should not normally be altered here. These two settings ensure that the size of the photo on all badges printed by this badge template are uniformly sized and have the same aspect ratio.

To accommodate minor variations in the aspect ratio of individual photos without distortion, enable the **Maintain Aspect Ratio** option.

See *Fields Common to All Objects* on the next page and *Fields Common to Picture and Graphic Objects* on page 408.

**Adding and Editing a Data Field Object**

1. Click **Add DB Field** to add a data field object to the canvas.
2. Click **Data Field** to hide or show the data field object settings.
3. In the **Data Field** drop-down list select a data field. For example, to have a badge include a person's name when it is generated, select one of the name fields listed, such as Full Name.
4. Adjust the appearance of the data field object. You can resize the object to ensure all text is visible as well as change the font, size, and color. Additionally, select the **Auto Resize** checkbox to make the text shrink to fit inside a fixed size box if the text in the specified font size does not fit. See *Fields Common to All Objects* on the next page and *Fields Common to Data Field and Text Objects* on the next page.

**Adding and Editing a Text Object**

1. Click **Add Text** to add a text object to the canvas.
2. Click **Text** to hide or show the text object settings.
3. In the **Text** field, enter the text you want to appear on all badges generated with this template.
4. Adjust the appearance of the database field object. You can resize the object to ensure all text is visible as well as change the font, size, and color. Additionally, select the **Auto Resize** checkbox to make the text shrink to fit inside a fixed size box if the text in the specified font size does not fit. See *Fields Common to All Objects* on the next page and *Fields Common to Data Field and Text Objects* on the next page.

**Adding and Editing a Graphic Object**

1. Click **Add Graphic** to add an image object to the canvas.
2. Click **#** or *Image File Name* item to show or hide the graphic object settings.
3. In the Image field, click **Choose File** to upload a file to the ACM system and add to the badge template.
4. Adjust the appearance of the photo object in various ways. See *Fields Common to All Objects* below and *Fields Common to Picture and Graphic Objects* on the next page.

**Fields Common to All Objects**

| Field | Description |
|---|---|
| **Layer Order** | A number indicating the order an object appears when objects are stacked in front of each other. The initial layer order is the order the objects were added to the template.<br><br>1 is the lowest layer, 2 is in front of 1 and so on. You can reorder the layers by typing over the value for each object. |
| **Location** | Click and drag the object on the canvas, or enter the horizontal and vertical coordinates of the top left corner.<br><br>The default setting of 0 x 0 would place the object in the top left corner, while 80 x 160 would place the object lower and to the right. |
| **Dimensions** | Modify the default size of the object (in pixels) if needed.<br><br>**Tip:** Do not modify the size of an identity photo object here. It is better to change the default values on the System Settings page, as this ensures the same aspect ratio is used for the dropping overlay when photos are taken with a badge camera and saved in the Identities database.<br><br>The first field is the width and the second field is the height. |
| **Rotation** | Select the number of degrees to rotate this object clockwise from the dropdown list.<br><br>The default is 0 degrees. |

**Fields Common to Data Field and Text Objects**

| Field | Description |
|---|---|
| **BG Color** | Click this field to choose a background color for the object. By default, it is set to be the same color as the badge template.<br><br>Use the color picker to either select a color from the palette or manually enter the color in RGB, HSV or hex code format. |
| **Opacity** | Enter how opaque you want the background color to be, in conjunction with the layer order.<br><br>0% is fully transparent and the default setting of 100% is fully opaque. |
| **Font** | Select the font you want for the text.<br><br>The font list includes text fonts and barcode fonts. Text fonts are listed first, then barcode fonts. |

| Field | Description |
|---|---|
| **Font Size** | Enter the font size in points. If Auto Resize is selected, this is the maximum font size. |
| **Auto Resize** | Select this checkbox to have the system automatically shrink the font size to fit the dimensions of the object. |
| **Alignment** | Select how you want the text to align inside the object. |
| **Text Color** | Click this field to choose a font color.<br><br>Use the color picker to either select a color from the palette or manually enter the color in RGB, HSV or hex code format. |
| **Opacity** | Enter how opaque you want the font color to be, in conjunction with the layer order.<br><br>0% is fully transparent and the default setting of 100% is fully opaque. |

**Fields Common to Picture and Graphic Objects**

| Field | Description |
|---|---|
| **Image** | (Applies to graphic objects only) Specifies the image to upload to the ACM system and place on the badge template. After the graphic is uploaded, the file name replaces **#** in the list of objects on the badge template. |
| **Maintain Aspect** | Check this box to always maintain the aspect ratio of the photo. When the aspect ratio is maintained, the photo is scaled to fit within the object space. If this option is disabled, the photo is automatically stretched to fill the object space. |
| **Border Width** | Select the border thickness (in pixels) for the picture or image from the drop-down list. The photo or graphic will be offset by the width of the border. |
| **Border Color** | Use the color picker to either select a color from the palette or manually enter the color in RGB, HSV or hex code format. |

**Adding a Barcode Using Static and Dynamic Objects**

1. When you create a badge template, you can add a barcode by using either of the following options:
   - Click **Add Text** to place a static barcode that will be the same for every badge that is generated from the template.
   - Click **Add DB Field** to place a dynamic barcode that changes to match the detail listed in the identity record.
2. After you add the badge object, select a barcode font. The available barcode fonts include **Barcode 3 of 9**, **Barcode 3 of 9 Extended**, **Aztec Code**, **Code One** and more. The font option lists the text fonts first and then the barcode fonts.
3. Click ✔ to save your changes and display the barcode in the preview area.

> **Note:** Many of these barcodes require a specific format or do not accept certain characters. If the data given to the barcode generator from the Identities database is invalid, the barcode will not be displayed on the badge.

## Badge Templates list

When you select

> **Badge Designer**, the Badge Templates list is displayed. From this page, you can add and edit badge templates with the Badge Designer.

Badge templates are used to define the layout of badges or cards that are used to access doors within your access control system. They are created by a qualified operator using the Badge Designer. Multiple badge templates can be defined in the ACM system.

This page lists all the badge templates that have been added to the system.

| Feature | Description |
|---|---|
| **Name** | The name of the badge template.<br><br>Click the name to edit the badge template. For more information, see *Using the Badge Designer* on page 403. |
| **Commands** | Click to delete the badge template. |
| | Click to copy the badge template.<br><br>The copy of the badge template is automatically added to the top of the list. |
| **Add Badge Template** | Click this button to add a new badge template. For more information, see *Using the Badge Designer* on page 403. |

# External Systems

Set up integration to cameras, sites and other third-party external systems.

> **Note:** Some external systems may not be available if your system does not have the required license.

Before you can connect and use the external systems, the external system must be installed and accessible to the appliance over the local network.

## Supported External Systems

Listed below are all the external systems that are supported by the ACM system. Some systems may not be available to you if your system does not have the required license.

- IP cameras and network video management systems (VMSs), including Avigilon Control Center.

  You can add individual cameras to add photos to the Identities database, or you can add whole network video systems that can be configured to work with doors and events in the ACM system, and record video triggered by events for surveillance.
- LifeSafety Power Supplies
- ViRDI Biometric Access scanners and readers
- Virtual Stations — ACM Verify™ Virtual Doors

  For example, the ViRDI external system requires a separate license. Before a ViRDI system can be created on your ACM server appliance, the system administrator for the ACM application must:

    - Add the ViRDI license to the ACM application. See *Adding a License* on page 357.
    - Add the four ViRDI-specific delegations to the role assigned to operators. These delegations are all prefixed with "ViRDI". See *Assigning Delegations to a Role* on page 84 and *Roles - Delegate page* on page 88.
- Bosch intrusion panels

  For more information, see *Bosch Intrusion Panels* on page 415.
- Allegion ENGAGE gateways

  For more information, see *IP/PoE Mode Installation* on page 266 and *Step 1: Creating an ENGAGE Site* on page 276.
- SALTO servers

  For more information, see *SALTO Door Installation* on page 281 and *Step 1: Connecting to a SALTO Server* on page 285.
- HID Origo

  For more information, see *Configuring HID Mobile Access® Credentials* on page 62 and *Step 1: Connecting to the HID Origo External System* on page 62.
- DMP intrusion panels

  For more information, see *DMP Intrusion Panel Installation* on page 424 and *Step 1: Connecting to a DMP Intrusion Panel* on page 426.

## Adding External Systems

You can add several types of external systems to the ACM system.

**Important:** Before you can add any external system, you must first connect a supported device to your network or server, and then configure the device as described in device documentation. Write down the device's IP address and onboard URL. For some external systems, refer to an ACM-specific integration guide that provides installation, connection and configuration instructions.

1. Select > **External Systems**.
2. Select the tab for the external system you want to add.
3. From the External Systems listing page, click or **Create** depending on the system.
4. In the following page, complete the required fields to add the new external system.
5. Click to save the new external system.

See also:

- *Step 1: Creating an ENGAGE Site* on page 276
- *Step 1: Connecting to a SALTO Server* on page 285
- *Step 1: Connecting to a DMP Intrusion Panel* on page 426

# Editing External Systems

1. Select > **External Systems**.
2. Select the tab for the type of external system you want to edit.
3. From the External Systems listing page, click the name or address of the specific system you want to edit.
4. In the following page, make the required changes.
5. Click to save your changes.

See also:

- *Editing an ENGAGE Site* below

## Editing an ENGAGE Site

To edit an ENGAGE site in ACM:

1. Select >**External Systems**.
2. Click the **Schlage** tab.
3. Click the site name.
4. Edit:

| | |
|---|---|
| **Site Name** | Up to 50 alphanumeric characters for the name of the site which represents the logical group of ENGAGE devices. Always create an ENGAGE site in the ACM application. A site that is already created in the ENGAGE application cannot be reused in the ACM application. In addition, a site cannot be used by more than one ACM appliance. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |

5. Click to save your changes.

   Click to discard your changes.

# Deleting External Systems

Uninstalling an external system does not remove it from your system. Uninstalling it will simply prevent communication with the ACM appliance. You may need to delete the external system as required.

1. Select > **External Systems**.
2. Select the tab for the type of external system.
3. Click next to the name of the external system.

   For Bosch intrusion panels, click . Associated items such as linkages and actions, and intrusion users will also be deleted.

   For DMP intrusion panels, click . Associated items such as linkages and actions, zones, areas, outputs, identity mapping, and intrusion users will also be deleted.

   For the HID Origo external system, click **Delete**.
4. When the confirmation message is displayed, click **OK**.

# External Systems - Integrating an ACM Appliance into an ACC™ Site

An ACM appliance can be integrated into an ACC site so that events occurring in the ACM software can trigger rules in the ACC software to initiate actions. For example, door events in the ACM software can trigger a rule that allows an ACC operator to grant door access, or an input event from a panic button or motion sensor in the ACM software can trigger a live camera feed, or video recording.

To integrate an ACM appliance, a special identity to interact with the ACC software must be created by an ACM administrator. This identity must be assigned a special role and delegation with specific rights, and a routing group that specifies the events that the ACC software receives. Only one identity must be created for this purpose.

As of ACM 5.10.10.2, a preconfigured role and delegation with the necessary rights are available for this special identity that is suitable for most integration scenarios. The role and delegation are both called **ACC Administrator**. However, if this special identity needs additional rights, you will have to modify the rights associated with the delegation, or configure a new role and delegation. The routing group has to be configured, and optionally if you plan to import Active Directory identities through ACM, you will have to configure remote authentication.

If you are using an earlier version of the ACM appliance, you will need to create your own ACC Administrator role and delegation with the appropriate rights.

Use the following steps to configure an identity to interact with the ACC software:

1. Ensure the **ACC Administrator** delegation has the following rights:
    - Appliance Listing
    - Delegations Listing
    - Doors Grant
    - Doors Listing
    - Force Password Change
    - Identities Listing
    - Identities Login - Remote
    - Identities Photo Render
    - Inputs Listing
    - Panels Listing
    - Partitions List
    - Roles Listing
    - Subpanels Listing
    - System Summary Listing
    - REST Appliance Status Display
    - REST Get Doors
    - REST Get Identities
    - REST Get Identity
    - REST Get Inputs
    - REST Get Panels
    - REST Get Right Groups
    - REST Get Roles
    - REST Get Subpanels
2. Create a routing group to define events sent from the ACM appliance to the ACC software.

a. Specify the following for the group:
   - **Schedule**: 24 Hours Active
   - **Schedule Qualifier**: Appliance
   - The **Installed** box must be checked

b. Add the following event types to the routing group:
   - Door held open
   - Forced Door
   - Intrusion
   - Invalid Credential
   - Maintenance
   - System
   - Tamper
   - Valid Credential

3. Create a role that allows the ACC software to communicate with the ACM system.
   a. Keep the default **Parent** value (none).
   b. Keep the default **Start Date** value (the current date).
   c. In the **Stop Date** box, enter an appropriate date for this role to expire. By default, the role will stop working 1 year from its creation date.
   d. Select the **Installed** checkbox and click **Save**.

      Additional tabs will appear.
   e. In the role's **Delegate** tab, assign only the **ACC Administrator** delegation that was created in the preceding steps.
   f. In the **Routing** tab, assign only the routing group that was created in the preceding steps.
4. If you plan to import Active Directory identities to the ACM appliance or the ACC software, configure a Lightweight Directory Access Protocol (LDAP) Collaboration. For Active Directory Remote Authentication, configure remote authentication from external domains.
5. Create a dedicated identity for interacting with the ACC software.

   **Note:** To protect the security of the connection between the ACM appliance and the ACC software, the dedicated identity should have only the permissions outlined in this procedure. Operators should not have access to this account.

   - Assign a **Last Name**, **Login**, and **Password** for the identity. Uncheck the **Force Password Change** checkbox. Do not enable MFA for the ACC user account.
   - The password should meet the minimum password strength requirements for your ACC site.

     The password strength is defined by how easy it is for an unauthorized user to guess. It is highly recommended that you select a password that uses a series of words that is easy for you to remember but difficult for others to guess.
   - Under the identity's **Roles** tab, assign only the role that was created in the preceding step.
6. If your ACM appliance uses partitions, add the identity as a member of the partitions they will need to access from the ACC Client.
7. Configure the ACM appliance to use the same NTP Time Server as the ACC Server.

   For Windows systems, the ACC Server gets its time from the operating system. For Avigilon Hardened

OS appliances, the NTP Time Server can be configured through the device's web interface.

a. In the top-right corner, click the gear icon to open the Setup & Settings menu and select **Appliance**.
b. In the **Time Server** box, enter the Time Server IP address.

Once these settings are applied, an ACC Client can connect to the ACM appliance. For more information, see the *ACC™ and ACM™ Unification Guide* (link).

# External Systems - Defining the Badge Camera for the System

Once all cameras or other imaging devices have been added as part of an external system, you can set which camera to use when creating badges for identities.

1. Select > **My Account**.
2. Under the Profile tab, select a camera from the **Badge Camera** drop down list:
   - **Local Camera** — Any camera connected directly to your computer or built into your computer or monitor.
   - **IP-based camera** — Any IP-based camera previously connected to your network and added to your ACM system.
3. When you're finished, click .

Next time you create a badge, the selected camera is used to take the identity photo.

# External Systems - ViRDI

When you select the **ViRDI** tab on the External Systems page, the ViRDI System Settings page is displayed. The ViRDI system allows you to use fingerprint readers for access control, and optionally to use additional authentication to provide two-way or three-way authentication for increased security. Only one ViRDI system setting can be configured on an ACM server appliance. If a replication server is deployed for this ACM server appliance, you can also configure ViRDI system settings for the replication server. After the ViRDI server is installed, ViRDI Biometrics tokens can be created for identities, and the Biometrics Enrollment Manager can be accessed to register fingerprints and additional authentication methods for ACM identities.

Two ViRDI readers are supported:

- ViRDI AC2000—supports fingerprint, or card and fingerprint authentication for up to 1,500 users.
- ViRDI AC5000 Plus —supports any combination of fingerprint, card, and PIN authentication for up to 20,000 users.

Fingerprints are registered using the ViRDI FOHO2 fingerprint reader, which can be installed at enrollment stations. The authentication method (one- two- or three-way authentication) used by the reader for these tokens is configured using the Biometrics Enrollment Manager (BEM).

## External Systems - ViRDI System Settings

When you click the **ViRDI** tab from the External Systems page, the ViRDI System Settings page is displayed.

This page allows you to create or delete the ViRDI system setting on an ACM server appliance.

| Feature | Description |
|---|---|
| **Appliance** | The appliance this server is connected to. |

| Feature | Description |
|---|---|
| **Reserved User ID Range** | The default minimum and maximum values are displayed. These values can be adjusted to meet the requirements of your system, but must be within the initial default range of 1 to 99999999.<br><br>Consider the following recommendations:<br><br>• Reserve a block of numbers within this range dedicated for ViRDI biometric tokens for use by the ACM system.<br>• Do not assign any of those numbers to physical cards for other types of access readers.<br>• Do not modify this range.<br><br>**Note:** If you must modify the range, contact Avigilon customer support for guidance. |
| **Web Service Port** | Accept the default port or enter a new port number.<br><br>If you change this port number from the default port (9875), you must also change the corresponding port number on every Biometric Enrollment (BE) Manager used for identity enrollment. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Delete** | Click to delete the server from the system. |
| **Update** | Click this button to add the ViRDI server to the system. |

# Bosch Intrusion Panels

The following procedures relate to Bosch intrusion panels.

## Integrating the ACM System with Bosch Intrusion Panels

Complete the following steps to integrate the ACM system with Bosch intrusion panels.

Requirements:

- ACM version 5.10.10 installed.
- ACM license for Bosch Intrusion.
- Bosch alarm panel B series (35xx, 45xx, 55xx, 85xx, 95xx) D9412, D7412.

Do the following to configure the Bosch alarm panel before you can connect to the ACM appliance:

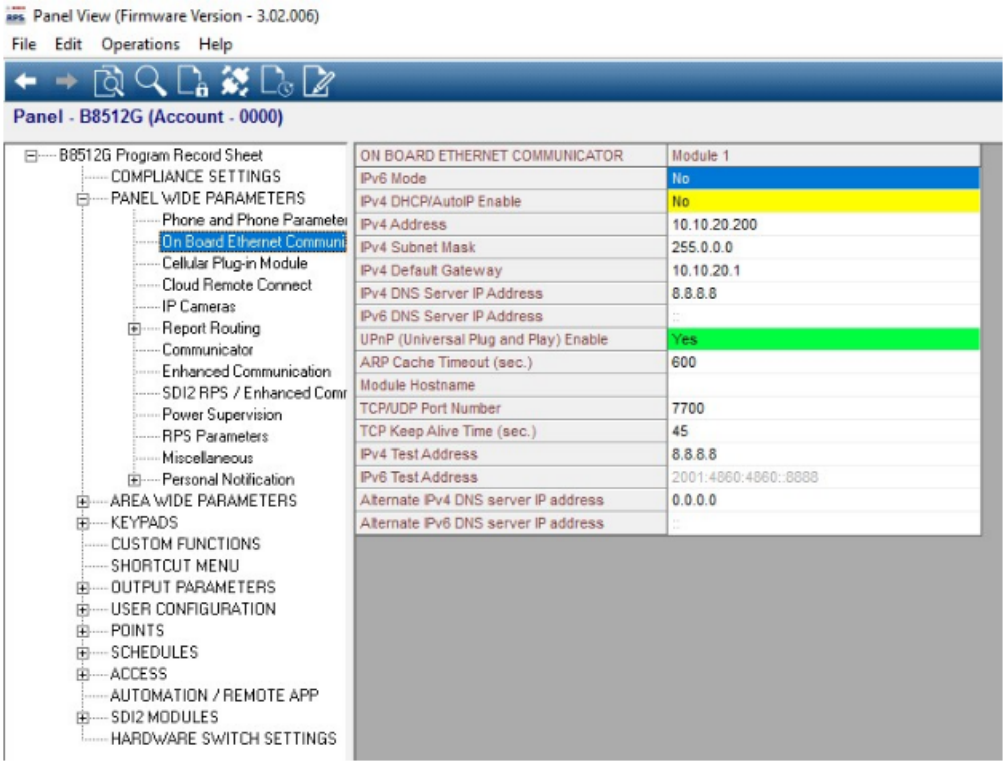
1. Download and install Bosch RPS (Remote Programming Software).

   More details about the software can be found at Bosch website: https://us.boschsecurity.com/en/products/intrusionalarmsystems/software/programmingsoftware/remoteprogrammingsoftware/remoteprogrammingsoftware_25629

   Depending on the alarm panel version (above B55xx Series) you will need the RPS dongle key (USB) to enable the software.
2. Launch the Bosch RPS software.

3. Do the following in RPS:
    - Go to the Panel View and select the panel connecting to the ACM appliance.
    - Select **AUTOMATION/REMOTE APP**.
    - Enter:
        - `Mode 2` in the **Automation Device** field.
        - `Bosch_Auto` in the **Automation Passcode** field. This password needs to be entered in the Automation Passcode field in the ACM application.
        - `Bosch_RSC` is the default in the **Remote App Passcode** field. This password needs to be entered in the Application Passcode field in the ACM application.
        - Save changes and upload to the panel.

4. Launch the ACM client and do the following:
    - Select **Settings** > **External Systems**. Click the **Bosch Intrusion** tab.
    - Click to add a new alarm panel.
    - Enter the **Panel Name**.
    - Enter the IP address in the **Address** field. Check that the IP address matches the IP address in RPS (see below).




- Enter the port number in the **Port** field. Make sure this matches the TCP/UDP Port Number in RPS (see above).
- Enter the **Automation Passcode** (same as the Automation Passcode in RPS).
- Enter the **Application Passcode** (same as the Remote App Passcode in RPS).
- Click the **Installed** checkbox.
- Click **Create** to save the configuration. After you save the configuration in the ACM software, it will take a couple of seconds to communicate with the alarm panel. You should see a green LED indicating “online." ACM imports all Areas, Users, Input, and Output data from the Bosch alarm panel.

## Adding a Bosch Intrusion Panel

To add a new Bosch intrusion panel:

1. Select > **External Systems**.
2. Click the **Bosch Intrusion** tab.
3. Click to add a new panel.
4. Complete the following fields:
    - Panel Name
    - Appliance
    - Address
    - Port
    - Automation Passcode
    - Application Passcode
    - Installed

5. Click **Create**.

> **Note:** The Areas, Points, Outputs and Users are created from the panel, as configured in Bosch's Remote Programming Software (RPS).

6. Click + beside the Panel name.
7. Select **Areas**. View the Area details.
8. Select **Points**. View the Point details.
9. Select **Outputs**. View the Output details.
10. Select **Users**. View the User details.
11. Click ✓ **Save**.

## Editing a Bosch Intrusion Panel

To edit and view a Bosch intrusion panel:

1. Select ⚙ > **External Systems**.
2. Click the **Bosch Intrusion** tab.
3. Review the panel status indicator to identify the current status of the panel.
4. Edit or view the following fields:
   - Panel Name
   - Appliance
   - Address
   - Port
   - Automation Passcode
   - Application Passcode
   - Installed
5. To view Area details, select **Areas**.
6. To view Point details, select **Points**.
7. To view Output details, select **Outputs**.
8. To view User details, select **Users**.

## Viewing Auto-Synced Bosch Intrusion Panels

If intrusion panel information is updated externally to the ACM system (e.g. new identities being added in Bosch's Remote Programming Software - RPS), the panel information is automatically synced in the ACM system.

1. Select ⚙ > **External Systems**.
2. Click the **Bosch Intrusion** tab.

   In ACM 6.34 and newer releases, ⚠ is no longer displayed for manual syncing. Allow a few seconds for the panel information to be automatically synced ( 🔄 ) in the ACM system.

## Deleting a Bosch Intrusion Panel

To delete a Bosch intrusion panel:

1. Select > **External Systems**.
2. Click the **Bosch Intrusion** tab.
3. Select the panel to be deleted.
4. Click to delete the panel.

> **Note:** The panel will be deleted and will disappear from this view.

## Viewing Bosch Intrusion Panel Areas

To view Bosch intrusion panel areas:

1. Select > **External Systems**.
2. Click the **Bosch Intrusion** tab.
3. Select a panel and click .
4. View the areas details that display.

> **Note:** Areas are not edited in the ACM system. All editing is done in Remote Programming Software (RPS) and updated through the panel.

## Viewing Bosch Intrusion Panel Points

To view Bosch intrusion panel points:

1. Select > **External Systems**.
2. Click the **Bosch Intrusion** tab.
3. Select a panel and click .
4. Select **Points**.
5. View the point details that display.

> **Note:** Points are not edited in the ACM system. All editing is done in Remote Programming Software (RPS) and updated through the panel.

## Viewing Bosch Intrusion Panel Outputs

To view Bosch intrusion panel outputs:

1. Select > **External Systems**.
2. Click the **Bosch Intrusion** tab.
3. Select a panel and click .
4. Select **Outputs**.
5. View the output details that display.

> **Note:** Outputs are not edited in the ACM system. All editing is done in Remote Programming Software (RPS) and updated through the panel.

## Viewing Bosch Intrusion Panel Users

To view Bosch intrusion panel users:

1. Select > **External Systems**.
2. Click the **Bosch Intrusion** tab.
3. Select a panel and click .
4. Select **Users**.
5. View the user details that display.

> **Note:** Users are not edited in the ACM system. All editing is done in Remote Programming Software (RPS) and updated through the panel. However, users can be associated to identities tokens. For more detail, refer to *Assigning Bosch Intrusion Panel Users to Identities* below.

> **Note:** It may take several minutes to retrieve user information from the panel.

### *Assigning Bosch Intrusion Panel Users to Identities*

Bosch intrusion panel users can be assigned to identities in the ACM system. This is done in order to allow users the ability to arm and disarm areas. This can be done:

- on a one-to-one basis (e.g. user 'Jane Smith' is associated to identity Jane Smith), or
- on a one-to-many basis (e.g. user 'Administration Team' is associated to identities Jane Smith, Robert Jones and Andrew Wilson).

To assign users to identities, do the following:

1. Select **Identities**.
2. Search for the required identity and select it from the list that displays. For more detail, refer to *Searching for an Identity* on page 64.
3. Click the **Tokens** tab.

> **Note:** In order to save the changes on this page ensure that the **Embossed Number** and **Internal Number** fields relating to the identity are completed.

4. In the **Intrusion Users: Available** the list select the user to add.

> **Note:** The list displays username, ID of the user and panel name for each user. These details are displayed to distinguish between users with the same or similar names.

5. Click ▶.

> **Note:** The username, ID of the user and panel name displays in the **Intrusion Users: Members** list. To remove an entry from this list, select the member and click ◀ to move the member to the **Intrusion Users: Available** list.

6. Click ✔.

## Supported Bosch Intrusion Panels

Noted below are the details of the supported Bosch Intrusion Panels:

| Panel | Details |
|---|---|
| **B3512** | Areas: 1<br>Custom Functions: 1<br>Keypads: 4<br>Events: 127<br>Passcode Users (+1 Installer): 10<br>Points: 16<br>Programmable outputs: 3<br>RF Points: 8<br>SKED Events: 1<br>Firmware version: 3.0.2 or greater |

| | |
|---|---|
| **B4512** | Areas: 2<br>Custom Functions: 2<br>Keypads: 8<br>Events: 127<br>Passcode Users (+1 Installer): 32<br>Points: 28<br>Programmable outputs: 27<br>RF Points: 20<br>SKED Events: 5<br>Firmware version: 3.0.2 or greater |
| **B5512** | Areas: 4<br>Custom Functions: 4<br>Keypads: 8<br>Events: 255<br>Passcode Users (+1 Installer): 50<br>Points: 48<br>Programmable outputs: 43<br>RF Points: 40<br>SKED Events: 5<br>Firmware version: 3.0.2 or greater |
| **B6512** | Areas: 6<br>Custom Functions: 6<br>Keypads: 8<br>Events: 1,000<br>Passcode Users (+1 Installer): 100<br>Points: 96 (8 on-board, 88 off-board and virtual)<br>Programmable outputs: 3<br>RF Points: 88<br>SKED Events: 6<br>Firmware version: 3.0.2 or greater |

| | |
|---|---|
| **B9512G** | Areas: 32<br>Custom Functions: 32<br>Keypads: 32<br>Events: 10,192<br>Passcode Users (+1 Installer): 2,000<br>Points: 599<br>Programmable outputs: 599<br>RF Points: 591<br>SKED Events: 80<br>Firmware version: 3.0.2 or greater |
| **B8512G** | Areas: 8<br>Custom Functions: 8<br>Keypads: 16<br>Events: 2,048<br>Passcode Users (+1 Installer): 500<br>Points: 99<br>Programmable outputs: 99<br>RF Points: 91<br>SKED Events: 40<br>Firmware version: 3.0.2 or greater |
| **D9412GV4** | Areas: 32<br>Custom Functions: 16<br>Keypads: 16<br>Events: 1,000<br>Passcode Users (+1 Installer): 999<br>Points: 246<br>Programmable outputs: 131<br>RF Points: 238<br>SKED Events: 40<br>Firmware version: Version 2.0 or greater |

| | |
|---|---|
| **D7412GV4** | Areas: 8<br>Custom Functions: 4<br>Keypads: 16<br>Events: 1,000<br>Passcode Users (+1 Installer): 399<br>Points: 75<br>Programmable outputs: 67<br>RF Points: 67<br>SKED Events: 40<br>Firmware version: Version 2.0 or greater |

# DMP Intrusion Panel Installation

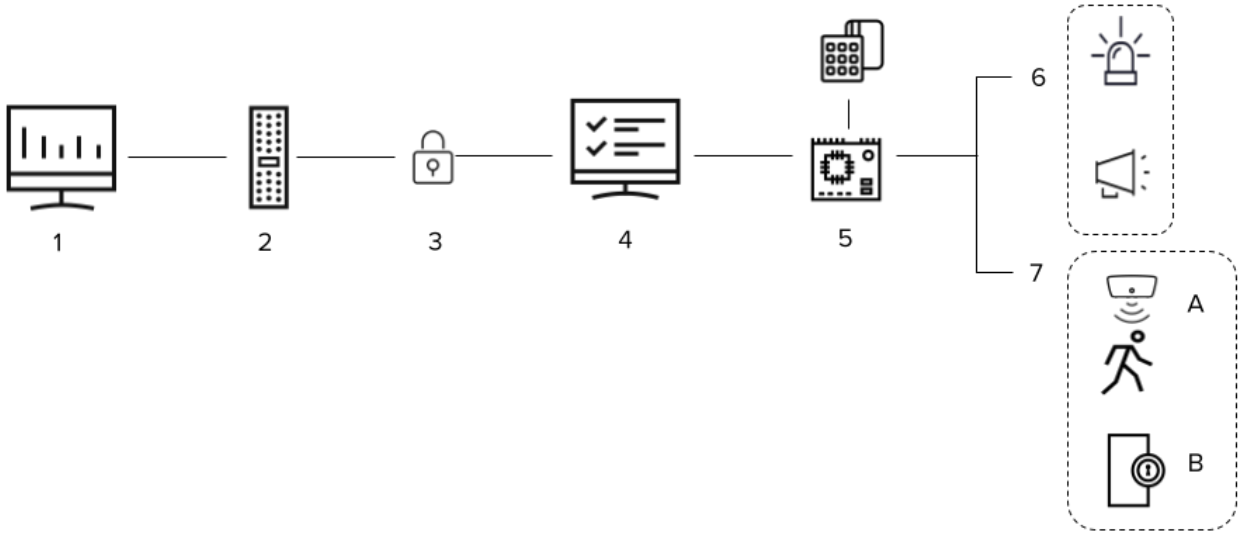
Add and configure Digital Monitoring Products (DMP) intrusion panels in ACM and monitor their areas, zones, outputs and DMP users. For more information, see:

- *System Overview* below
- *Prerequisites* on the next page
- *Supported Devices* on page 426
- *Step 1: Connecting to a DMP Intrusion Panel* on page 426
- *Step 2: Viewing an Installed DMP Intrusion Panel and its Areas, Zones, Outputs and Users* on page 428
- *Step 3: Assigning DMP Intrusion Users to Identities* on page 428

**Note:** Before you begin, configure the DMP intrusion panel using the DMP Remote™ Link software before you use the ACM system. Every time you add, update or delete panels in the DMP intrusion system, the updates are automatically synced with ACM. Areas, zones, and outputs are not edited in the ACM system. All editing is done in the Remote Link software. Identities (and their tokens) must be managed in the ACM system.

## System Overview

**Figure 20:** ACM system organization for DMP intrusion panel and devices




| | |
|---|---|
| 1 | ACM applications, including identity (badging), administration, video surveillance and alarm monitoring |
| 2 | ACM appliance |
| 3 | Encrypted connection provided by the ACM appliance certificate |
| 4 | DMP Remote Link software for the configuration of areas, zones, outputs and users |
| 5 | DMP intrusion panel and keypad, including panel battery power, AC power, tamper switch, two phone lines, wireless sensor, and printer, if installed |
| 6 | Outputs, including smoke detectors and fire alarms (graphic annunciators), if installed |
| 7 | Areas, including devices that are connected to multiple zones (A, B), if installed<br>For example, zone A can be connected to a wireless sensor and zone B can be connected to a keypad on a door. |

## Prerequisites

Contact your integrator to purchase a 1-panel or 10-panel license. More than one license can be installed on an ACM appliance.

**Note:** For general, new, or updated instructions about the installation and configuration of the DMP intrusion system and DMP Remote Link software, refer to DMP system documentation. DMP firmware version 212, or newer, is required. DMP rights are not honored in ACM. ACM 6.34, or newer, is required.

### *Remote Link Software Configuration*

In the Remote Link software, save the following DMP panel configuration.

### A.C. Power Failure Notification

Optional. To change the default A.C. power failure notification setting (default is 1 hour):

1. Go to **Program** > **System Options**.
2. Set **Power Fail Delay** to **0** to receive an event in a few seconds or choose the number of hours.
3. Save the setting.

### Panel Encryption

Required. To enable panel encryption:

1. Go to **Program** > **Remote Options**.
2. Enter a checkmark in the **Encrypt Network Remote** checkbox.
3. Save the setting.

### Remote Key

Required. To define the remote key for the panel:

1. Go to **Program** > **Remote Options**.
2. Enter the value in **Remote Key**.

   **Note:** The Remote Key must be entered in the ACM application.

3. Save the setting.

## Supported Devices

The ACM application is mapped to the physical configuration of DMP intrusion systems as follows.

| Door | Panel | Subpanel | External System |
|---|---|---|---|
| See external system | See external system | - | Up to 100 XR150 and XR550 Series intrusion panels in any combination to each license<br><br>Support for areas, zones and other items is dependent on the panel model. See vendor documentation for the limits. |

## Step 1: Connecting to a DMP Intrusion Panel

**Note:** Before you begin, make sure the DMP intrusion panel is connected to the local network.

To add a DMP intrusion panel in ACM:

1. Select ⚙ > **External Systems**.
2. Click the **DMP Intrusion** tab.
3. Click **Add**.
4. Enter:

| | |
|---|---|
| **Panel Name** | A unique name for the panel. Choose a name that will help you identify the devices it controls. Duplicate names are not allowed.<br><br>**Important:** Make sure the encryption setting is enabled in the Remote Link software. For more information, see *Prerequisites* on page 425. |
| **Panel Type** | Read-only field. The type or model of DMP intrusion panel. |
| **Appliance** | Read-only field. The name of the ACM appliance that is connected to the panel. |
| **Address** | The IP address or hostname of the panel. |
| **Port** | The TCP/IP port number configured on the panel. |
| **Account Number** | The account number of the panel. |
| **Remote Key** | The remote key configured in the Remote Link software. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition. |
| **Installed** | Enables communication between the ACM appliance and panel after saving. |

5. Click the **Create** button.

   All areas, zones, and outputs are imported in an installed state from the online panel.

Next, see *Step 2: Viewing an Installed DMP Intrusion Panel and its Areas, Zones, Outputs and Users* on the next page.

### *Deleting a DMP Intrusion Panel*

To delete a DMP intrusion panel:

1. Select ⚙ > **External Systems**.
2. Click the **DMP Intrusion** tab.
3. Select the panel to be deleted.
4. Click 🗑.

   **Note:** Associated items such as linkages and actions, zones, areas, outputs, identity mapping, and intrusion users will also be deleted.

5. Click **OK**.

### Step 2: Viewing an Installed DMP Intrusion Panel and its Areas, Zones, Outputs and Users

On the DMP Intrusion tab of the external system, do any of the following:

- Type the name of the object in the filter box ( ) to filter the list.
  Click the column heading to sort the list.
- If an area, zone, or output should not be monitored, uninstall it by removing the checkmark.
  The status changes to No in the Installed column.
- Allow a few seconds for the panel information to be synced ( ) in the ACM system.

Next, see *Step 3: Assigning DMP Intrusion Users to Identities* below.

### Step 3: Assigning DMP Intrusion Users to Identities

Assign DMP intrusion users to the tokens of their identities in the ACM system to enable the arming and disarming of the intrusion system.

**Note:** A token can be mapped to only one intrusion user per panel.

1. Select **Identities** > **Identities** and click **Search** to select an identity already created.
   If you need to add an identity, see *Adding an Identity* on page 65.

   **Tip:** Identities are defined by their DMP user name, ID and DMP panel name.
2. Click the **Tokens** tab.
3. In the **Available** list, move the identities to the **Members** list.
4. Click .

### Generating Reports

To generate the Event Report for intrusion systems:

1. Select **Reports** > **Reports**.
2. Click **Event Report**.
3. Click and to add items to **Find**.
   Include **Intrusion DMP**.
4. Click to save the search.

### Enabling Debug Logs

**Note:** Enabling the appliance logs requires these delegations: Appliance Log, Appliance Log

Download, Appliance Log Show, and Appliance Log Update. Contact your support representative to enable the Debug checkbox, if needed.

To debug using the appliance logs:

1. Select > **Appliance** and the **Access** tab.
2. Put a checkmark in the **Debug** checkbox next to **Intrusion Service**.
3. Click .

See also *Accessing Appliance Logs* on page 353.

# Maps

Maps are a graphical representation of your access control system. Import maps of your facility and populate them with door, panel, subpanel, input, output, camera and global action alarm points that can be monitored.

## Creating a Map

Maps help you visually locate where doors, cameras, inputs, and outputs are located in your facility. You can use any image in BMP, GIF, JPEG, PNG, or PDF files.

Maps also display Mustering dashboard elements. For more information about setting up a Mustering dashboard, see *Mustering - Creating a Dashboard* on page 321.

1. Select > **Maps**.
2. To add a new map, click **Add Map Template**.
   a. Enter a name for the map.
   b. Do one of the following:
      - To upload the image file for the map, click **Choose File** and then click **Open**.
      - To not use a background, select **Blank Canvas**.
   c. Click **Save**.

## Editing a Map

Edit a map after you save a new map template for the first time or from the list of map templates.

- On the right is the base map image. You can move map items anywhere in this work area.
- On the left are the map properties, including the name and size. In the Map Details area are a list of all the items that can be added to the map.

## Configuring the Map Background

1. Edit any of the following fields.

| | |
|---|---|
| **Name** | The name of the map. |
| **File** | The base map image. |
| **Blank Canvas** | Check this box to leave the map background white. |
| **Size** | The width and height of the map in pixels. |
| **Partitions** | Displayed for a partitioned ACM appliance only. To restrict operator access to the item, select one or more partitions. To allow all operators access to the item, do not select a partition.<br><br>**Note:** It is recommended that you do not assign maps to a partition. If you add a device to the map that is part of multiple partitions, the map may generate an error when a user without the same permissions as the device tries to use the map. |

2. Click ✔ to save.

## Adding Items to the Map

1. In the Map Details area, click the **Add** button beside the item you want to add.
2. Move the icon to where it should appear in the map.

**Tip:** Map icons are added on top of each other in the top left corner of the map. Move added icons right away or you may lose track of all the items that have been added to the map.

## Setting the Icon Size

1. Select a field in the following table.
2. Select **Small**, **Medium**, **Large**, or **Extra Large** in the **Size** field.
3. Click to save.

| Field | Icon | Field | Icon |
|---|---|---|---|
| **Doors** | | **Cameras** | |
| **Panels** | | **Zoom In** | |
| **Supbpanels** | | **Zoom Out** | |
| **Inputs** | | **Global Actions** | |
| **Outputs** | | **Dashboard Elements** | Square, circle, or text object |

## Showing or Hiding Items

- Click the or beside each item.
  If any of the item lists are empty, you need to add or configure that item first.

## Deleting Items

- Click beside the listed item.

## Configuring the Mustering Dashboard Element

1. Enter a title for the dashboard element. The map is updated.
2. Click the **Title Font Color** field to change the text color.
3. In the **Title Font Size** drop down list, select the size. The options are Small, Medium and Large.
4. For the **Opacity** option, choose how transparent you want the dashboard element to be. You can enter a percent number, or move the slider to set the opacity. 100% is opaque and 0% is transparent.
5. In the **Location** field, enter where you want the dashboard element to appear on the map. You can also move the dashboard element directly on the map.

6. In the **Element Type** drop down list, select if you want the dashboard element to appear as Text Only or Graphic & Text.

   If you choose Graphic & Text, the following options are displayed:

   a. In the **Area Group/Area** drop down list, select the muster area this dashboard element represents. You can select a specific area or a group of areas.
   b. From the **Graphic Shape** drop down list, select Circle or Square.
   c. Click the **Graphic Color** field to change the graphic shape color.
   d. For the **Graphic Size** option, choose how big you want the graphic to be. You can enter the size in pixels, or use the slider to adjust the size.

# Linking Maps

Use the **Zoom In** and **Zoom Out** to link a map with less detail (a building or campus) to a map with more detail (a floor or room).

## Example Use

An operator has detected an alarm in a building. Their monitor displays the building map, showing the alarmed point, but they need to get a closer look to confirm the exact position of the alarm. To do this, they click , which is linked to a floor map. The floor map appears with a closer view of the alarmed point. After they have taken care of the alarm, they can then click to return to the general building map and resume general surveillance.

# Using a Map

Access a map of your site, facility or floor plan from the Monitor page to do any of the following:

- Monitor the status of doors, panels, subpanels, inputs and outputs that are installed. For example, a mustering station on the third floor of a building.
- Set the door mode and door commands on the map.

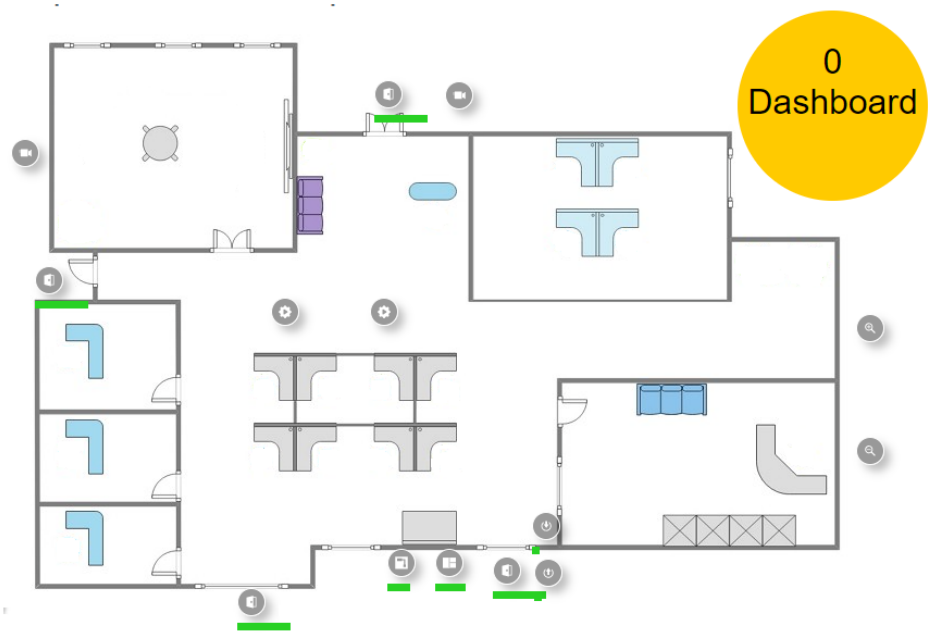
  > **Note:** Unlike the Physical Access > Doors or Monitor > Dashboard page which displays all modes and commands regardless of door type, the Monitor > Maps page displays only the modes and commands that are supported by your door or device.

- Keep track of identities as they arrive at muster stations from the Mustering dashboard.

## Viewing a Map

To access and monitor your site from a map:

1. Select **Monitor** > **Maps**.
2. In the Map Templates list, click **Show** next to the name of a map.
   Some of the displayed elements may not appear in your map or the example below.




> **Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.

| Field | Icon | Field | Icon |
|---|---|---|---|
| **Doors** | | **Cameras** | |
| **Panels** | | **Zoom In** | |
| **Supbpanels** | | **Zoom Out** | |
| **Inputs** | | **Global Actions** | |
| **Outputs** | | **Dashboard Elements** | Square, circle, or text object |

## Hardware Status

The following indicators are displayed on the map as events occur:

| Icon | Status | Description |
|---|---|---|
| | Green bar | The hardware is operating normally. |
| | Red square | The hardware is in an alarm state. The counter in the square shows the number of unacknowledged events. |
| | Solid blue disk | An active override is in effect on the door. |
| | Hollow blue disk | An inactive override is defined. |
| | Red bounding box around the status bar | The door is in Priority Mode. |

## Map Actions

The actions you can complete on a map are determined by the permissions of your assigned roles.

| To... | Do this... |
|---|---|
| Review hardware status | The colored bar below each item displays an overview of the current communication and power status.<br>• Click the icon on the map to display the control menu.<br>For more information about the colored hardware status bar, see the specific hardware status page. For more information about the status colors, see *Status Colors* on page 43. |
| Review an alarm | If you see a red alarm indicator, the item on the map is in an alarm state.<br>• Click the alarm indicator to see the status details.<br>For more information about alarm actions, see *Monitoring Alarms* on page 34. |
| Modify or delete an override | If you see solid blue disk indicator, an active override is in effect on the door. If you see a hollow blue disk indicator, an inactive override is defined.<br>• Click the indicator to open the Doors: Overrides page to see details. |
| Respond to a priority situation | If you see a red bounding box around the status indicator, the door is in Priority Mode.<br>**Important:** A door is in Priority Mode when a priority situation has been declared at your site. All doors affected by the situation are placed into Priority Mode and only the Priority ACM Operator, responsible for dealing with priority situations can interact with the door. |

| To... | Do this... |
|---|---|
| Control a door | Click on the map to display the control menu for the selected door.<br><br>**Note:** Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.<br><br>Use the menu options to set the Door Mode. For more information, see *Door Modes* on page 203.<br><br>Use the following menu options to mask or unmask alarms:<br>• **Mask Held** — Mask the Door Held Open Alarm.<br>• **Unmask Held** — Unmask the Door Held Open Alarm.<br>• **Mask Forced** — Mask the Door Forced Open Alarm.<br>• **Unmask Forced** — Unmask the Door Forced Open Alarm.<br><br>To view live video, recorded video, notes, instructions, identities, and history click **Trace** to display the event transactions for the door.<br><br>To hide the control menu, click the icon again. |
| Control a panel or subpanel | Click or on the map to display the panel control menu, and then for the panel or subpanel use these options:<br>• Panels<br>  ◦ **Download Params** — Download the latest system configurations to the panel.<br>  ◦ **Tokens** — Download the tokens to the panel.<br>  ◦ **Reset/Download** — Reset and download the current system configuration to the panel.<br>  ◦ **APB Reset** — Resets all panel and area counts to zero.<br>  ◦ **Clock** — Re-sync the panel time.<br>  ◦ **Trace** — Display the event transactions for the panel.<br><br>**Note:** This is the only option supported for ASSA ABLOY IP panels.<br><br>• Subpanels<br>  ◦ **Trace** — Display the event transactions for the subpanel.<br><br>Viewing live video, recorded video, notes, instructions, identities, and history can be performed on the event transactions.<br><br>To hide the control menu, click the icon again. |

| To... | Do this... |
|---|---|
| Control an input | Click the on the map to display the input control menu for the input.<br>Use these options to mask or unmask the input:<br>• **Mask** — Mask the input.<br>• **Unmask** — Unmask the input.<br>To hide the control menu, click the icon again. |
| Control an output | Click the on the map to display the output control menu for the output.<br>Use these options to initiate output actions:<br>• **On** — Activate the output.<br>• **Off** — Deactivate the output.<br>• **Pulse** — Pulse the output.<br>To hide the control menu, click the icon again. |
| Display video | Click the on the map to display the Camera Video window. |
| Open a linked map | Click to display a linked map, or to display a linked map. |
| Monitor the dashboard | If there is a Mustering dashboard configured on the map, it may appear as a line of text or as a shape with text inside.<br>The dashboard displays the number of identities in the area and may include the name of the area. In *Using a Map* on page 432, the dashboard is the gray square.<br>Click the dashboard to see a list of all the identities that are in the area. Click outside the pop-up dialog to hide the identities list. Click the First Name or Last Name to view the identity. |

# Assets

Upload sound files and configure them to play when alarm events occur on panels, subpanels, doors, and more.

- *Uploading Sound File* below
- *Assigning Sounds to Alarm Events* on the next page
- *Turning Sound On/Off* on page 39

**Note:** Only sound files in WAV or MP3 format are supported. When playing sounds, ensure the audio on your device or machine is enabled.

## Uploading Sound File

To upload sound files:

1. Select > **Assets**.
2. Click the Add Sound Asset button.
3. Click **Choose File**, select the custom sound file, and click **Open**.
4. Enter a **Name**. The filename is used, if a name is not entered.
5. Click **Save**.

### Playing Sound Files

- Click next to the sound file.

### Deleting Sound Files

- Click next to the sound file.

For the next step, see *Assigning Sounds to Alarm Events* below.

## Assigning Sounds to Alarm Events

To assign sounds to alarm events:

1. Go to any of the events pages:
   - **Physical Access** > **Events** for a list of global events. Select an event name.
   - **Physical Access** > **Doors** or **Monitor** > **Dashboard** > **Doors** for local door events. Select a door name, the **Events** tab, and then **Create Local** next to a global event.
   - **Physical Access** > **Panels** or **Monitor** > **Dashboard** > **Panels** for local panel events. Select a panel name, the **Events** tab, and then **Create Local** next to a global event.
   - **Physical Access** > **Panels** for local subpanel, input, or output events. Select a panel name and then the **Events** tab. Click + next to Hardware Selector to view the nested list of subpanels, inputs, and outputs. Select a subpanel name, input name, or output name, and then **Create Local** next to a global event.
   - **Monitor** > **Dashboard** > **Supbpanels**, **Inputs**, or **Outputs**. Select the ... button to the right of the subpanel, input, or output name, and then select **View**. Select the **Events** tab and then **Create Local** next to a global event.
2. Ensure the **Alarm** checkbox is selected for the event type.

   For more information, see *Adding Event Types* on page 384.
3. In **Alarm Sound**, select a sound.

   **Note:** A default beeping sound is played, if no sound is selected.
4. Click **Save**.

For the next step, see *Turning Sound On/Off* on page 39.

# Priority Situations

For Mercury Security doors.

Your site may have requirements for your ACM system to support your organization's emergency procedures. Typical emergency procedures might be for potentially life-threatening situations (such as fires, tornadoes, earthquakes, physical attacks), and hazardous situations (such as chemical spills, gas leaks, explosions). Your ACM appliance can provide automated access control of doors connected to Mercury panels in unpredictable emergency and high-priority situations, including lockdowns and evacuations, to support your organization's existing operating procedures.

**Important:** The functionality to respond to high-priority situations is not supported by HID® VertX® panels. If you only have HID VertX doors at your site, the procedures provided for high-priority situations using the ACM system do not apply. If you have a mix of HID VertX and Mercury Security doors, do not include HID VertX doors in any group of doors that are associated to your Priority Door Policies or Priority Door Global Actions.

If you have Mercury Security doors operating with SimonsVoss SmartIntego wireless locks, refer to SimonsVoss SmartIntego documentation. The ACM lockdown priority operation is superseded by the Escape and Return state of the SimonsVoss wireless lock when it becomes engaged in a lockdown situation.

To respond to a priority situation a **Priority ACM Operator** activates a **Priority Door Policy**, which is a specialized Door Policy that is configured to immediately apply a **Priority Mode** to a group of doors upon activation. Optionally, the policy can also set the Door Mode of all the doors to a single value, such as Door Locked No Access for an emergency lockdown.

While a door is in Priority Mode, it is highlighted in red wherever it appears in the ACM client, such as the Doors listing page and on maps or dashboards. These doors can be controlled only by Priority ACM Operator, who have a **Priority Role** that allows them this control. A Priority ACM Operator can issue commands to individual doors in Priority Mode to allow safe exit of trapped people, to allow emergency responders in, or to isolate persons of interest, and so on.

**WARNING —** Risk of loss of functionality. While a priority situation is active, any configuration change made to the ACM system may have unintended consequences. To avoid this risk during an active priority situation, do not allow any ACM operator other than the Priority ACM Operator to make (or approve) any configuration changes, including changes in unaffected partitions. For more information, see on page 444

Upon deactivation of the policy, the Priority Mode is removed and the doors return to the door mode they are configured to be in at the time. To secure this functionality from unauthorized access, it can all be isolated in a secure **Priority Partition**.

## Planning Priority Door Policies

Analyze all existing door policies at your site before designing and configuring any Priority Door Policies. You must be familiar with all the door policies that are configured at your site. The settings in all of your non-

priority and priority door policies must be designed, configured, and tested to ensure that there are no unexpected results after these polices are applied over each other in all possible combinations.

For example, a Priority Door Policy is configured that overwrites only a subset of the door settings. Some of those settings are set in the base configuration of a door, and some are reset by the non-priority door policy that is normally in effect at the time the Priority Door Policy is activated. After the priority situation is over and the Priority Door Policy is deactivated, the currently scheduled non-priority policy is re-activated and applies its settings.

The priority door policies or other related priority items you configure to support them in the ACM system must be:

- Aligned with the emergency procedures in effect at your site.
- Securely isolated so that they cannot be interrupted by lower priority activities.
- Regularly tested and rehearsed to ensure they function as expected, and corrected if they do not.

**Note:** You can configure **Priority Door Global Action** pairs. However, Priority Door Global Actions are not recommended; see *Limitations of Priority Global Actions* on page 445. Priority Door Global Actions are specialized Global Actions for doors (the first Priority Global Action applies a Priority Mode, and optionally sets the door mode to a single known value, to a group of doors upon activation, and the second Priority Global Action restores those doors to the mode they are configured to be in at the time).

If you have previously used a pair of Global Actions to respond to a priority situation, consider replacing them with a single Priority Door Policy, as recommended.

**Important:** A Priority Door Policy is the most secure way to control access with the ACM system in an emergency situation. It is also more robust than a Priority Door Global Action. A Priority Door Policy will stay in effect on the doors it is installed on even if:

- The ACM appliance:
  - Is restarted
  - Is disconnected from power
  - Fails over to a backup appliance
- The door or door panel:
  - Goes offline
  - Is rebooted
  - Is disconnected from power
  - Is disconnected from the access control network.

## Priority Door Policies, Global Actions, and Modes

When activated, a Priority Door Policy or Priority Door Global Action sets all doors in an associated group of

doors into Priority Mode. Additionally, it can set all these doors to a single configurable door mode (for example, Locked - No Access) regardless of their current mode when activated.

While a Priority Door Policy or Priority Door Global Action active, only Priority ACM Operator is authorized to issue commands to doors in Priority Mode can change the door mode on specific doors (for example to allow safe exit of trapped people, to allow emergency responders in, or to isolate persons of interest). After the situation is resolved, you can remove the Priority Door Policy or Priority Door Global Action and all the doors will return to the mode they normally are in at the current time.

Priority Door Policies and Priority Door Global Actions and the associated door Priority Mode are at the top of the ACM system's priority hierarchy. For information about the priority hierarchy, see *Priority Hierarchy* on page 446.

A Priority Door Policy is created in the same way as any other door policy, with specific settings that define it as a Priority Door Policy. A Priority Global Action is created in the same way as any other global action, except that it can only be configured for the Door Mode.

# Priority Door Policies and Emergencies

Use Priority Door Policies to support your organization's critical emergency response procedures, which might include lockdowns and evacuations.

To ensure the security of Priority Door Policies, isolate everything required to manage the Priority Door Policy in a Priority Partition, accessible only to the Priority ACM Operator responsible for managing the ACM system during an emergency.

The operators, roles and groups associated with Priority Door Policies must be configured to conform to your organization’s operating procedures:

- Roles to trigger a Priority Door Policy, and the assignment of those roles to operators, must be defined so that the policy can be activated only in conformance with those operating procedures.
- Door groups that are affected by a Priority Door Policy must be defined so that they cannot be inadvertently altered.

Secured priority situation response functionality is configured in the following order:

1. **Priority Partition**: A specialized partition that isolates all the functionality required for a secured response to a priority situation.
2. **Priority Role**: A specialized role for authorized ACM operators responsible for operating the ACM system during priority situations. The Priority Role must be assigned the following delegations:
    - **Policies Set Priority** to configure a Priority Door Policy.
    - **Global Action Set Priority** to configure a Priority Global Action.
    - **Doors Commands During Priority** to allow manual control of doors in Priority Mode during a priority situation
3. **Priority ACM Operator**: An ACM operator authorized to operate the ACM system during emergencies. This operator is assigned membership of the:
    - Priority Role
    - Priority Partition
4. **Priority Group**: A Group that is a member of the Priority Partition that is reserved to associate doors with Priority Door Policies.

5. **Priority Door Policy**: A specialized Door Policy that enables the **Priority Mode** and, optionally, a single known value for the Door Mode, to be assigned to a group of doors upon activation. A door in Priority Mode is highlighted in red wherever it appears in the ACM client, such as the Doors listing page and on maps, while a Priority Door Policy is in effect.

For the procedure on securely isolating a Priority Door Policy, see *Configuring a Secure High-Priority Emergency Response* below.

# Configuring a Secure High-Priority Emergency Response

You can maximize the security of your high-priority emergency response procedure by isolating everything it requires the ACM system to manage in a dedicated partition, referred to as a Priority Partition. If your site:

- Does not use partitions, you only need to create one Priority Partition.
- Does use partitions, you should determine how many Priority Partitions you require. Whether you need more than one Priority Partition depends on the complexity and requirements of your organization. Consider:
    - One Priority Partition for your entire site.
    - Several Priority Partitions that do not correspond to the existing ones.
    - A matching set of one Priority Partition for each existing partition.

It is recommended that you define as few Priority Partitions and Priority Door Policies as possible. For example, do not configure multiple Priority Door Policies with the same settings in the same Priority Partition.

To secure your high-priority emergency response using a Priority Partition, complete the following steps:

1. Create a partition, and give it a name that identifies it clearly as the Priority Partition.
2. Add all the doors at your site that you want to control in any emergency or high-priority situation as members of the Priority Partition. Typically this would be all the doors managed by the ACM system.
3. Create a Priority Role for the Priority ACM Operator and add the following delegations as members:
    - **Policies Set Priority**: Allows the identity to configure a Priority Door Policy.
    - **Global Action Set Priority**: Allows the identity to configure a Priority Global Action.
    - **Doors Commands During Priority**: Allows the identity to use commands to change the attributes of a door in priority mode.

    **WARNING —** Assign these three delegations only to the Priority Role reserved for Priority ACM Operator.
4. Add a new identity, and give it a name that identifies it clearly as the Priority ACM Operator. Assign the high-priority identity as a member of the:
    - Priority Role
    - Priority Partition

    Alternatively, you can add an existing administrator identity as a member of the Priority Role and the Priority Partition, although this will be less secure.

    **WARNING —** Risk that users other than the Priority ACM Operator can change door modes when a Priority Door Policy is in effect. Users with the Doors Commands During Priority delegation can use commands to change the door mode. To avoid this risk, assign the Doors Commands During Priority delegation only to the Priority Role and assign the Priority Role only to the high-priority ACM system administrator.
5. Create a group, and give it a name that identifies it clearly as the Priority Group. Assign the Priority Group to the Priority Partition.

6. Create a Priority Door Policy. Assign the Priority Door Policy to the Priority Partition.
7. A Priority Door Policy is created in the same way as any other door policy, with the following five specific settings on the **Mercury** tab:
    a. Set the **Lock Function** to **None**.
    b. Set **Custom Schedule** to **24 Hours Active**.

       The **Priority** checkbox is enabled.

       You can use a custom schedule other then the recommended **24 Hours Active**. However, the intent of a Priority Door Policy is that it should be used on demand, not on a schedule. When you set the Custom Schedule option for a Priority Door Policy, be aware of the following:
        - Holiday and custom schedules must be configured with matching values for the Type option so that they can interact.
        - **Do not** set Custom Schedule to Never Active. With this setting, the doors affected go into Priority Mode when the policy is activated, but their door mode is not updated with the value in the policy.
        - **Do not** associate a Priority Door Policy with a schedule that has fixed start and end times. The purpose of a Priority Door Policy is to respond to an unanticipated situation when it occurs and to stay in effect until the situation is resolved. A Priority Door Policy is intended to be activated on demand only.
        - The maximum number of custom schedules is 255 if you use a custom schedule other than 24 Hours Active.
    c. Click the **Priority** checkbox.
    d. Use the **Door mode** option to set the mode for all doors to have when this policy is active. For example **Locked No Access** for a policy tor a lockdown, or **Unlocked** for a policy for an evacuation. Leave this option blank if you want to individually reset each door's mode from its normal mode after the policy is activated.
    e. Set the **Offline Door Mode** to the same value as the **Door Mode**. This ensures that, if the door is disconnected from network or power during the emergency, the door mode will remain in the same as the mode set by the Priority Mode while the door is disconnected, or after power is restored.

       **CAUTION —** Set the offline door mode to match the priority mode. This ensures that the door stays in the same mode in the event of a subpanel going offline or the subpanel is uninstalled while the Priority Door Policy is in effect.
    f. Optionally, if there are additional settings that must be retained on all the doors affected by this policy, ensure they are correctly configured. For example, if there is a door policy that contains settings for other options that must be retained through an emergency, and that policy might be installed on these doors at the time of the emergency.
8. Create two Global Actions: to activate the Priority Door Policy, and to deactivate the Priority Door Policy. Assign the Global Actions to the Priority Partition.

   Create the Global Actions with the following specific settings:
    a. Assign each global action to the Priority Partition.
    b. Set **Type** to **Policy Install/Un-install**.
    c. Set the **Sub-Type** to:
        - **Install** for the global action to activate the Priority Door Policy
        - **Un-install** for the global action to deactivate the Priority Door Policy
    d. In each global action, add the Global Door Policy as the only member.
9. Create a new map template. Place the door icons and global actions created in the previous steps on the map. Assign the map to the Priority Partition.
10. In the Priority Group, associate the Priority Door Policy with all the doors in the Priority Partition.

# Testing a Secure Priority Emergency Response in the ACM System

To test that all of your emergency-related configurations and activities are securely isolated:

1. Log out of the ACM client.
2. Log in as the Priority ACM Operator.
3. Activate the Priority Door Policy:
    a. Navigate to the priority map.
    b. Click on the icon for the global action to activate the Priority Door Policy.
4. Verify that the doors enter into Priority Mode:
    - On the priority map, a red bounding box appears over the status bar under each door icon. Hover the mouse over the status bar to see the **Door in Priority mode** tooltip.
    - On the Doors listing page, all users will see a red bounding box over each door in Priority mode. Commands to change the door made are enabled for the Priority ACM Operator.
5. Log out as the Priority ACM Operator and log in as an ACM client user who is not a member of the Priority Partition, and verify that the user:
    - Can see:
        - On any map other than the priority map, a red bounding box over the status bar under the door icon for any door in Priority Mode on that map. Hover the mouse over the status bar to see the **Door in Priority mode** tooltip.
        - On the Doors listing page, a red bounding box over each door in Priority mode. All commands that affect doors are disabled for the user.
    - **Cannot** see any of the members of the Priority Partition:
        - The Priority Door Policy on the Policy list
        - The two policy install/uninstall global actions for the Priority Door Policy on the Global Actions list.
        - The priority group on the Groups list.
        - The map template on the Maps list or the Monitor > Maps page.
    - **Cannot** initiate any door commands on any door in priority from the Doors list.
6. Log in as the Priority ACM Operator.
7. Deactivate the Priority Door Policy:
    a. Navigate to the priority map.
    b. Click on the icon for the global action to deactivate the Priority Door Policy.
8. Log out as the Priority ACM Operator and log in as an ACM client user who is not a member of the Priority Partition, and verify that the user:
    - Can see:
        - On any map other than the priority map, that there is no red bounding box over the status bar under the door icon for any door that was in Priority Mode on that map.
        - On the Doors listing page, there is no red bounding box over each door in Priority mode.
    - Can initiate any door commands on any door from the Doors list according to their role.

# Activating the High-Priority Emergency Response

Several techniques can be used to make it as easy as possible for authorized personnel to trigger a Priority

Door Policy in the event of an emergency.

A Priority ACM Operator can trigger the installation of priority-enabled policy in response to an emergency, from an ACM monitoring station:

- From the Policies list, click in the Installed column next to the name of the Priority Door Policy for the type of emergency.
- From the map associated with the Priority Partition, click on the global action icon for installing the Priority Door Policy for the type of emergency.

You can also configure or install ways for other users to trigger an emergency response by the ACM system using Global Linkages. For example you can:

- Issue priority emergency badges to security personnel to swipe at any card reader.
- Install panic buttons wired in to the access control system at strategic locations.

These configurations are complex and should be planned and completed by a skilled security professional with detailed knowledge of the ACM system.

# During a High-Priority Situation

There are several actions that the Priority ACM Operator must complete immediately after a Priority Door Policy is installed to ensure that the priority policy is not interrupted while it is in effect:

- Check that there are no scheduled jobs running or about to start and if there are, stop them from running or starting.

  **WARNING —** Risk that doors in priority mode can be returned to the mode they normally are in at the current time while a Priority Door Policy or Priority Global Action is in effect. A scheduled job or global linkage that affects a door panel (such as a door install or uninstall, door grant, panel install or uninstall, policy install or policy uninstall, and others) will terminate a Priority Door Policy or Priority Global Action on the doors affected by the interruption. A door bulk update will also terminate a Priority Global Action. To avoid this risk, stop any scheduled job or global linkages from running or starting, during the emergency.
- Verify that there are no global actions or global linkages about to be initiated.
- Verify that there are no other users with any of the high-priority delegations active during the emergency situation. The only exception might be if your organization requires the deployment of more than one Priority ACM Operator working in coordination.

  **WARNING —** Risk that users other than the high-priority ACM system administrator can change door modes when a Priority Door Policy is in effect. Users with the Doors Commands Set Priority delegation can use commands to change the door mode. To avoid this risk, assign the Doors Commands Set Priority delegation only to the Priority Role and assign the Priority Role only to the high-priority ACM system administrator.
- Secure the ACM appliance to ensure that it does not accidentally reboot.
- If you are using peer-to-peer or hot standby replication , issue all commands from the same appliance from which the Priority Door Policy or Priority Door Global Action was issued.

During the emergency, the Priority ACM Operator can use the ACM client to issue commands to individual doors in Priority Mode. This allows the Priority ACM Operator to grant access to emergency responders, provide safe exits for trapped people, or isolate persons of interest.

If there are ACM system partitions not affected by the active Priority Door Policy, normal operations can

continue in those partitions.

While a Priority Door Policy is active, the Priority ACM Operator must ensure that the Priority Partition is isolated and all activities affecting the ACM system are under strict control. In the Priority Partition:

- **Do not** allow anyone other than the Priority ACM Operator to use the ACM client in the Priority Partition, and limit the number of people using the ACM client in any other partitions (if any).
- **Do not** activate additional Priority Door Policies.

  **WARNING —** Risk of unpredictable results installing multiple Priority Door Policies. If you install a second Priority Door Policy while one is already in effect, the latest created policy takes precedence, which may not be the most recently installed policy. To avoid this risk, never activate a second Priority Door Policy until after the first policy is deactivated.
- **Do not** allow any configuration, maintenance, or scheduled maintenance operations.
- **Do not** activate any Priority Door Global Actions.

The Priority Door Policy is active until it is deactivated. Deactivation restores doors to their normal door mode for the current time.

# Deactivating a Priority Door Policy

The ability to end a Priority Door Policy must be restricted to ensure that your site is fully secured before normal access is restored. The Priority ACM Operator is responsible for deactivating the Priority Door Policy after it is determined that the emergency situation has been resolved and it is safe to return the ACM system to its normal operating state.

The deactivation of an active Priority Door Policy can only be completed from an ACM monitoring station, regardless of how the policy was triggered:

- From the Policies list, click in the Installed column next to the name of the active Priority Door Policy.
- From the map associated with the Priority Partition, click on the global action icon for uninstalling the active Priority Door Policy.

# Limitations of Priority Global Actions

Priority Global Actions are not recommended for emergency situations. A Priority Door Global Action is much less robust than a Priority Door Policy. Never use a Priority Door Global Action while a Priority Door Policy is activated.

**WARNING —** There is a risk that, while a Priority Global Action is in effect, doors in priority mode can be returned to the mode they normally are in at the current time. Any action that interrupts the functioning of the ACM appliance or the door panels will terminate a Priority Global Action on the doors affected by the interruption. Some examples of actions that can cause this are:

- Failover of the ACM appliance
- Reboot of the ACM appliance or a door panel.
- Network disconnection, or a site-wide power recycling or outage.
- Change to any door attribute on the Doors editing page while a door is in priority mode.
- Reset/Download from the Panel Status page.
- Scheduled job or global linkage for a door bulk update.

**WARNING —** There is a risk that not all doors in a large number of doors set to Priority Mode will correctly return to their normal operating state when a Priority Global Action is used to restore a large number of doors. To avoid this risk, when you define a Priority Global Action for doors, also define a group of doors containing all the doors associated with that Priority Global Action, and then to restore the doors to their normal operating state:

- Navigate to the Doors listing page.
- Filter the list of doors by the group associated with the Priority Global Action.
- Select all the doors in the group.
- Click the **Door Action** button and select **Restore** from the drop-down list.

**WARNING —** Risk of unpredictable results using Priority Global Actions in either a peer-to-peer replication or hot-standby environment:

- Priority Global Actions executed on one appliance are not mirrored on the other appliance. When a global action is executed on one appliance, it only affects the doors that are connected to that appliance.
- While a Priority Global Action is in effect, and there is a failover to the hot-standby appliance, affected doors can be returned to the mode they normally are in at the current time.

To avoid these risks, use a Priority Door Policy. Priority Door Policies installed on one appliance in either a peer-to-peer replication or hot-standby environment are mirrored on the other appliance.

# Priority Hierarchy

There are three priority levels for door mode changes in the ACM software. Within each level, the possible actions also have an order of precedence. A change to a door state that has a higher priority and precedence than the change that defined the current state takes effect whenever it is activated. A change with a lower priority and precedence than the change that defined the current state will never take effect. Changes with equal priority and precedence take effect in the order they are made.

Commands such as Grant issued directly in the ACM client have the highest priority, and can be activated at any time. For example, during a lockdown priority situation, when all doors are automatically locked, the Priority ACM Operator can grant access to specific doors from the Maps page or the Door list page for first responders.

| Priority | Type of Change | Act On | Operator Rights Required |
|---|---|---|---|
| **Highest** | UI commands on doors in priority state | Single door in the affected group of doors | Rights on a priority status door |
| | Active Priority Door Policy | Predefined group of doors associated with the policy | |
| | Active Priority Global Action | Predefined group of doors associated with the global action | |

| Priority | Type of Change | Act On | Operator Rights Required |
|---|---|---|---|
| **Medium** | UI Commands with rights on a non-priority status door | Single door in a non-priority state | Rights on a non-priority status door |
| | UI Commands without rights | | None |
| | Wireless door lock function | Wireless lock functions | |
| | **Note:** The ACM lockdown priority operation is superseded by the Escape and Return state of the SimonsVoss wireless lock when it becomes engaged in a lockdown situation. | | |
| | The above three Medium priority changes supersede each other when sequentially applied. Any one of them will supersede an Override command. | | |
| | Override | | |
| **Low** | Custom Schedule<br>Non-priority Door Policy<br>Non-priority Door Global Action<br>Macro/Trigger<br>Base Mode<br>Job Specification (two global actions)<br>Door template | | |

# Triggering Door Lockdown By Panic Button or Red Card

Mercury Security doors only.

To set up a panic button or red card that locks down a door in a high priority situation and releases the locked door after the lockdown issue is resolved:

1. Add a **Policy** to trigger the panic button and add another policy to release it.

   Example:

   | Name |
   |---|
   | Lockdown policy install |
   | Lockdown policy uninstall |

   For more information, see *Adding a Policy* on page 90.

2. Panic button only. Choose a method to associate each policy with the subpanel, input or output.
   - Add a **Global Action** to activate the panic button and add another global action to deactivate it. Associate those actions with the policy by moving them to the **Members** list.

     Example:

     | Name | Type | Sub-Type | ▶ Members |
     |---|---|---|---|
     | Global action name install | **Policy Install/Un-Install** | **Install** | Policy name |
     | Global action name uninstall | **Policy Install/Un-Install** | **Un-Install** | Policy name |

     For more information, see *Adding Global Actions* on page 315.
   - Add a **Global Linkage** to associate each policy with the input or output on the **Actions** tab by moving them to the **Members** list.

     Example:

     **Actions** tab:

     | Name | ▶ Members |
     |---|---|
     | Linkage name install | Global action name install |
     | Linkage name uninstall | Global action name uninstall |

3. Red card only. Add a **Global Linkage** to associate each lockdown policy with an identity and its token on the **Devices**, **Events** and **Tokens** tabs. Move the input or output, door event and token to the **Members** list.

   Example:

   **Devices** tab:

   | Name | Type | ▶ Members |
   |---|---|---|
   | Linkage name install | **Door** | Input on subpanel *N* Address *N* |
   | Linkage name uninstall | **Door** | Input on subpanel *N* Address *N* |

   **Events** tab:

   | Name | ▶ Members |
   |---|---|
   | Linkage name install | **Local Grant - not used** |
   | Linkage name uninstall | Choose an event to release the locked door |

   **Tokens** tab:

   | Name | Type | ▶ Members |
   |---|---|---|
   | Linkage name install | **Door** | Input on subpanel *N* Address *N* |
   | Linkage name uninstall | **Door** | Input on subpanel *N* Address *N* |

4. When a lockdown situation arises, activate the lockdown policy for the panic button or red card by pressing the panic button or swiping the red card on the reader, respectively.
5. When the lockdown situation is resolved, deactivate the lockdown policy.

   On the Policies list, click ✔ next to the lockdown policy.

   Example:

   | Name |
   | --- |
   | Lockdown policy uninstall |

   For more information, see *Policies list* on page 91.

# Overriding Door Modes and Schedules

**Note:** Overrides are only supported on Mercury panels using firmware 1.27.1 or later. Your current version of the ACM software includes compatible firmware you can download to your panels. You can create up to 100 overrides on a single panel.

Use overrides to apply a temporary one-time change to the normal door mode of a selected set of doors. For example, to extend or delay opening or closing hours, or for closing on a snow day. Overrides can be scheduled to take effect immediately, or in advance (for example, for a one-time occurrence such as an all-access event next week in a normally locked room). When an override ends, the door or doors each return to the mode they are supposed to be in according to their schedule at that time. Overrides are not recurring. For almost all purposes, an override should be deleted as soon as it has ended as there is a maximum number of overrides per panel.

Override functionality is designed to work best with your regular door schedules. Overrides have a medium priority-level in the ACM priority hierarchy and many higher-priority actions take precedence. For more information about this hierarchy see *Priority Hierarchy* on page 446. For example a manual command to a specific door, or a priority lockdown command to a set of doors, takes precedence. If a priority lockdown occurs while an override is in effect, the priority lockdown becomes active. After the priority lockdown has been cleared by the Priority ACM Operator, the override becomes active on the doors if it is still in effect, otherwise each door returns to its regular schedule for that time.

On Mercury panels using firmware earlier than 1.29, an override starts and ends at the beginning of the minute of its scheduled time. On Mercury panels using firmware 1.29 or later, an override starts at the beginning of the minute and ends at the end of the minute of its specified time. Time overlaps are not supported. For example, you can specify 1:00 - 1:30 and 1:31 - 1:59 overrides.

**Important:** You can only add an override to doors you are authorized to access that are on the same ACM server. However, you can modify or delete any override, and your changes will apply to all the doors in the override, including doors you are not normally authorized to access. If partitioning is used in your ACM system and you expect users authorized for specific partitions to modify an override, define individual overrides for each partition rather than a single override that spans multiple partitions. Otherwise, users can modify overrides that affect doors they cannot see and be unaware of any changes.

## Adding an Override

You add an override by selecting a set of doors on the Door  list, clicking the Override control button, specifying the door mode, and the start and end times of the override.

To add an override:

1. Select **Physical Access**.
2. Click the checkbox for each door you want to add to the override.

   If you want to override all the doors you can see in your system, click **All** at the top of the left column to select all the doors.

3. Click **Override**.
4. Select the door action or door mode you want applied to all the doors in the override:
   - **Disabled** — Stops the doors from operating and allows no access.
   - **Unlocked** — Unlocks the doors.
   - **Locked No Access** — Locks the doors.
   - **Facility Code Only** — This door can be accessed using a facility code.
   - **Card Only** — This door can be accessed using a card. No PIN is required. See *Appendix: pivCLASS Configuration* on page 503.
   - **Pin Only** — This door can only be accessed by entering a PIN at a keypad. No card is required.
   - **Card and Pin** — This door can only be accessed using both a card and a PIN.
   - **Card or Pin** — This door can be accessed either by entering a PIN at a keypad or by using a card at the card reader.

   **Note:** The Pin Only and Card or Pin door modes are not available if the Allow duplicate PINs option has been selected on the System Settings - General page.

5. Specify the date and time settings for **Start Day/Time** and **End Day/Time**. Both are required. Time is specified to the minute. On Mercury panels using firmware earlier than 1.29, the override begins and ends at the beginning of the minute you specify. On Mercury panels using firmware 1.29 or later, an override starts at the beginning of the minute and ends at the end of the minute of its specified time. Time overlaps are not supported. For example, you can specify 1:00 - 1:30 and 1:31 - 1:59 overrides.

   **Tip:** To start an override immediately, click **Now** in the **Start Day/Time** pop-up window.

   **Important:** The date and time the override is active is based on the settings at the controller panel for the doors, not the ACM server. If your ACM server is in a time zone ahead of the time zone of your ACM client and the doors and panels you control, you may see an error message that the override occurs in the past. You can ignore this error message if your settings in the local time zone are correct.

6. Add an optional note to provide relevant information for future use.
7. If partitions are used, you can restrict the override to only those doors in the Doors Selected list that are in a specific partition.
8. Click **Add**.

# Accessing the List of Overrides

You can access a list of all overrides from the Doors page:

- Click **Overrides:** (above the list of doors) to open the **Doors: Overrides** page for all defined overrides.

> **Tip:** The total number of defined overrides is displayed next to Overrides:.

You can access a list of all overrides for a specific door from the Doors page.

- A blue disk in the **Override** column for a door indicates overrides are defined for the door. The disk has two states:
  - ●: An override is currently active.
  - ○: An override is defined, but not active. An inactive override can be an override that has been completed but not deleted, or an override that has not yet started.
- Click the disk to open the **Doors: Overrides** page listing all the overrides for that door.

> **Tip:** Completed overrides must be manually deleted. Overrides are intended to be temporary actions for use on an as-needed basis. Most overrides should be deleted as soon as they are completed and no longer needed. Keep only override definitions that are highly likely to be re-used as defined, with only the start and end time and date settings modified.

For more information, see *Modifying and Deleting Overrides* below.

# Monitoring Overrides

Use the Maps feature to monitor overrides on doors. When a door that is displayed on a map is included in an override, the status indicator for the door is updated to display a blue disk. The disk indicates overrides are defined for the door. The disk has two states:

- ●: An override is currently active.
- ○: An override is defined, but not active. An inactive override can be an override that has been completed but not deleted, or an override that has not yet started.

For example, if an override is active on a door, a solid blue disk is displayed next to the green bar:

For more information, see *Using a Map* on page 432.

# Modifying and Deleting Overrides

On the **Doors: Override** page you can select an override to modify or delete overrides.

**To modify the override:**

1. Click on the override name in the **Name** column to open the Override: Edit page.

   If partitions are used, and doors you cannot see are included in the override "One or more doors in this override are in partitions you cannot see. These doors will be affected by your changes if you continue." is displayed. You can modify all the override settings, but only add or remove doors that you are authorized to see.
2. Make the modifications you need.
   - All settings can be modified if partitions are not used in your ACM system.
   - In the Doors Selected section, you can add doors to the override by highlighting them in the **Available** list and moving them to the **Members** list.
3. Click **Save**.

**To edit the base settings of any door in the override:**

- Click on the door name in the **Selected** column.

  Changes made to the base settings do not take effect until the override expires.

**To delete an override:**

- Click .

  The time the override is deleted is logged by the system. When an active override is deleted, the door or doors each return to the mode they are supposed to be in according to their schedule at that time.

# Modifying an Override

To modify the override:

1. Select the door action or door mode you want applied to all the doors in the override:
   - **Disabled** — Stops the doors from operating and allows no access.
   - **Unlocked** — Unlocks the doors.
   - **Locked No Access** — Locks the doors.
   - **Facility Code Only** — This door can be accessed using a facility code.
   - **Card Only** — This door can be accessed using a card. No PIN is required. See *Appendix: pivCLASS Configuration* on page 503.
   - **Pin Only** — This door can only be accessed by entering a PIN at a keypad. No card is required.
   - **Card and Pin** — This door can only be accessed using both a card and a PIN.
   - **Card or Pin** — This door can be accessed either by entering a PIN at a keypad or by using a card at the card reader.

   **Note:** The Pin Only and Card or Pin door modes are not available if the Allow duplicate PINs option has been selected on the System Settings - General page.

2. In the Doors Selected section, add doors to the override by highlighting them in the **Available** list and moving them to the **Members** list.

   **Important:** If partitions are used, only doors that are not in any partition or are in the partitions you are authorized to see are displayed in the Doors Selected list.

3. Specify the date and time settings for **Start Day/Time** and **End Day/Time**. Both are required. Time is specified to the minute. On Mercury panels using firmware earlier than 1.29, the override begins and ends at the beginning of the minute you specify. On Mercury panels using firmware 1.29 or later, an override starts at the beginning of the minute and ends at the end of the minute of its specified time. Time overlaps are not supported. For example, you can specify 1:00 - 1:30 and 1:31 - 1:59 overrides.

   **Tip:** To start an override immediately, click **Now** in the **Start Day/Time** pop-up window.

   **Important:** The date and time the override is active is based on the settings at the controller panel for the doors, not the ACM server. If your ACM server is in a time zone ahead of the time zone of your ACM client and the doors and panels you control, you may see an error message that the override occurs in the past. You can ignore this error message if your settings in the local time zone are correct.

4. Add an optional note to provide relevant information for future use.
5. If partitions are used, you can restrict the override to only those doors in the Doors Selected list that are in a specific partition.
6. Click **Save**.

# Setting Personal Preferences

To set up your personal preferences, select > **My Account** from the top-right. Navigate through the tabbed pages and edit the details as required. The tabbed pages include:

- **Profile:** use this page to edit your account details and preferences.
- **Batch Jobs:** use this page to view the batch jobs that have been run from your account.
- **Job Specification:** use this page to add, edit, activate/ deactivate, or delete batch jobs.

## Changing the Password in My Account

While you are logged in to the ACM system, you can choose to change your password any time.

1. In the top-right, select > **My Account**.
2. On the Profile tab, enter your current password in **Old Password**.
3. In **Password**, enter your new password.

   As you enter your new password, the status bar underneath will tell you the strength of your password. Red is weak, while green is very strong. Use a combination of numbers, letters, and symbols to increase the password strength. The password must be at least 4 characters long.
4. Click **Save**.

   A system message tells you that you will be logged out.
5. When the login screen appears, log in with your new password.

## Setting Your Preferred Language

To set your preferred language in the ACM system:

1. Select > **My Account**.
2. Select the language in **Locale**.
3. Click **Save**.
4. Log out and log back in.

> **Note:** The online help is provided only in English (US), French, German, Italian and Spanish. If you set your system to a language other than these five languages, English (US) online help will be the default.

## Scheduling Batch Jobs

Batch jobs are processes, such as generating reports, that are performed automatically, according to a

schedule.

From the Job Specification page, you can create the following batch jobs:

## Generating a Batch Report

Batch reports are custom reports generated on a schedule and which can contain more data than reports generated from the Reports  list, the Report Edit page or from the Report Preview page.

There are no length limits on any batch reports generated in the CSV spreadsheet format. In PDF format, the Audit Log report is limited to 13,000 records, the Identity Summary Report is limited to 100,000 records, and the Transaction Report is limited to 50,000 records.

**WARNING —** Risk of system becoming unusable. Scheduling large reports on separate but overlapping schedules, may cause memory problems that can result in the ACM system being unusable. To avoid this risk, schedule the start times for large reports, such as audit logs in any format, to allow for each report to finish before the next starts.

Perform this procedure to generate a custom report on a schedule.

1. Select >**My Account** and click the Job Specification tab.

   The Job Specification page is displayed.

2. Click the **Add** button.

   The Job Specification - General dialog box is displayed.
3. In the **Appliance** drop down list, select the appliance on which this job will run.

   Only those appliances previously defined for this system appear in this option list.

   If only one appliance is used for this system (the default), this field is automatically populated.
4. In the **Name** field, enter a name for this batch job.
5. From the **Type** drop down list, select **Report**.

   After you select the job type, additional options are displayed.
   - From the **Report** drop down list, select the report you want to batch.

     Only custom reports appear in this list.
   - From the **Output Format** drop down list, select the format in which you want this job generated.
6. Click **Next**.

   The following screen shows the select report definition. Click **Back** to select a different report.
7. Click **Next** to continue.
8. On the following page, select how often the batch report is generated. From the **Repeat** drop down list, select one of the following options:
   - **Once** —- The report will be generated once. Click the **On** field to display the calendar and select a specific date and time.
   - **Hourly** — The report will be generated at the same minute of every hour. Enter the minute when the report is generated at each hour. For example, if you want the report generated at 1:30, 2:30, etc. then you would enter `30`.
   - **Daily** — The report will be generated every day at the same time. Enter the specific time when the report is generated in 24 hour time format.
   - **Weekly** — The report will be generated each week on the same day and time. Select the checkbox for each day the report will be generated, and enter the specific time in 24 hour format.

- **Monthly** — The report will be generated each month on the same day and time. Select the days when the report is generated and enter the specific time in 24 hour format. `Shift` + click to select a series of days, or `Ctrl` + click to select separate days.

9. Click **Next**.

   A summary is displayed.

   Select the **Send Email** checkbox if you want to receive an email copy of the report after it has been generated. In the following field, enter your email address.

10. Click **Submit** to create this job.

11. To activate or deactivate this job, select the job and click **Activate/Deactivate**

## Applying an Identity Profile to a Group Using a Job Specification

Create and schedule an Identity Update batch job to apply a new, updated or temporary identity profile to all of the identities in a predefined group.

> **Note:** Not all identity fields are supported in identity profiles.

After you make changes to an identity profile, the identities previously created from the identity profile are not automatically updated. Using a job specification and scheduling the job is one of the ways that these changes can be applied.

Scenarios to apply an identity profile to a group of identities include:

- To apply a set of standard settings. When you have many identities defined with non-standard settings, create a group containing these users and a new profile containing the standard settings. Then apply the new profile to the group of identities.
- To apply modified settings in a commonly used identity profile. After you make changes to an identity profile, the identities created from the identity profile are not automatically updated. You need to create a batch job to apply these changes. Create a group of all the users that were created using this profile, and then apply the modified profile to that group. If the profile is frequently modified, you can create a repeating schedule.
- To apply a profile temporarily to a group. When you have identities that require a different profile for a short time that cannot be cannot be satisfied using a policy, you can use an Identity Update batch job to "turn on" a temporary profile for a specified duration, and then "turn off" that profile by replacing it with a permanent profile. If the temporary profile is used repeatedly in a predictable manner, you can create a repeating schedule.

> **Note:** A group containing all of the identities previously created from the identity profile must be created before the changes can be applied to the group. If the required groups have not been created, contact your System Administrator.

When you choose to create an Identity Update job, you have the option to apply a new, updated or temporary identity profile to the group.

A temporary door template is one that is applied for a specific period of time (either once or repeating) You can apply a temporary door template to a group by using the Off Identity Profile option. Once the new identity profile expires, the original identity profile is applied.

To create an Identity Update job specification:

1. Select > **My Account** and click the Job Specification tab.

   The Job Specification page is displayed.

2. Click the **Add** button.

   The Job Specification dialog box is displayed.

3. In the **Appliance** drop down list, select the appliance on which this job will run.

   Only those appliances previously defined for this system appear in this option list.

   If only one appliance is used for this system (the default), this field is automatically populated.

4. In the **Name** field, enter a name for this batch job.
5. From the **Type** drop down list, select **Identity Update**.

   After you select the job type, more options are displayed.

   - From the **Group** drop down list, select the group of identities that you want to change.
   - From the **Identity Profile** drop down list, select the identity profile that you want to apply to the group. If you are applying a temporary profile, this is the "on" profile.
   - From the **Off Identity Profile** drop down list, select the identity profile to be applied if you want an identity profile applied temporarily (that is, you want the identity profile to expire).
   - From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.

6. Click **Next** to continue.

   The Job Specification - Schedule dialog box is displayed.

7. From the **Repeat** drop down list, select how often this batch job is run. Then specify the time you want the profile to be applied. If you selected an Off Identity Profile, you also specify when the Off profile is applied.

   - **Once** —- The batch job is run once. Click the **On** and **Off** fields to display the calendar and select a specific date and time.
   - **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter `30`.
   - **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.
   - **Weekly** — The batch job is run each week on the same day and time. Select the checkbox for each day the job will run, and enter the specific time in 24 hour format.
   - **Monthly** — The batch job is run each month on the same day and time. Select the days when the job will run and enter the specific time in 24 hour format. `Shift` + click to select a series of days, or `Ctrl` + click to select separate days.

8. Click **Next**.

   A summary is displayed.

9. Click **Submit** to create this job.
10. To activate or deactivate this job, select the job and click **Activate/Deactivate**.

## Applying a Door Template to a Group Using a Job Specification

For ASSA ABLOY, Avigilon and Mercury Security doors.

Create and schedule a Door Update batch job to apply a new, updated or temporary door template to all of the doors in a predefined group.

After you make changes to a door template, the doors previously created from the door template are not

automatically updated. Using a job specification and scheduling the job is one of the ways that these changes can be applied.

Scenarios to apply a door template to a group of doors include:

- To apply a set of standard settings. When you have many doors defined with non-standard settings, create a group containing doors and a new template containing the standard settings. Then apply the new template to the group of doors.
- To apply modified settings in a commonly used door template. After you make changes to a door template, the identities created from the door template are not automatically updated. You need to create a batch job to apply these changes. Create a group of all the doors that were created using this template, and then apply the modified template to that group. If the template is frequently modified, you can create a repeating schedule.
- To apply a template temporarily to a group. When you have doors that require a different template for a short time that cannot be cannot be satisfied using a policy, you can use an Identity Update batch job to "turn on" a temporary template for a specified duration, and then "turn off" that template by replacing it with a permanent template. If the temporary template is used repeatedly in a predictable manner, you can create a repeating schedule.

**Note:** A group containing all of the doors previously created from the door template must be created before the changes can be applied to the group. If the required groups have not been created, contact your System Administrator.

When you choose to create a Door Update job, you have the option to apply a new, updated or temporary door template to the group.

A temporary door template is one that is applied for a specific period of time (either once or repeating). You can apply a temporary door template to a group by using the Off Door Template option. Once the new door template expires, the original door template is applied.

To create a Door Update job specification:

1. Select > **My Account** and click the Job Specification tab.

   The Job Specification page is displayed.

2. Click the **Add** button.

   The Job Specification - General dialog box is displayed. All options marked with * are required.
3. In the **Appliance** drop down list, select the appliance on which this job will run.

   Only those appliances previously defined for this system appear in this option list.

   If only one appliance is used for this system (the default), this field is automatically populated.
4. In the **Name** field, enter a name for this batch job.
5. From the **Type** drop down list, select **Door Update**.

   After you select the job type, additional options are displayed.
   - From the **Group** drop down list, select the group of doors that you want to change.
   - From the **Door Template** drop down list, select the door template that you want to apply to the group.
   - From the **Off Door Template** drop down list, you have the option to select to an alternative

door template when the first door template expires.

- From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.

6. Click **Next** to continue.

   The Job Specification - Schedule dialog box is displayed.

7. Select how often this batch job is run. From the **Repeat** drop down list, select one of the following options:

   If you selected an Off Door Template, you will have the option to enter when the Off template is applied. Otherwise, only the On field is displayed.

   - **Once** —- The batch job is run once. Click the **On** field to display the calendar and select a specific date and time.
   - **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter `30`.
   - **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.
   - **Weekly** — The batch job is run each week on the same day and time. Select the checkbox for each day the job will run, and enter the specific time in 24 hour format.
   - **Monthly** — The batch job is run each month on the same day and time. Select the days when the job will run and enter the specific time in 24 hour format. `Shift` + click to select a series of days, or `Ctrl` + click to select separate days.

8. Click **Next**.

   A summary is displayed.

9. Click **Submit** to create this job.
10. To activate or deactivate this job, select the job from the list in the Batch Job Specifications window and click **Activate/Deactivate**.

## Scheduling a Global Action

Perform this procedure to schedule global actions.

> **Note:** The global actions must be created before they can be scheduled. If the required global actions have not been created, contact your System Administrator.

1. Select **>My Account** and click the Job Specification tab.

   The Job Specification page appears.

2. Click the **Add** button.

   The Job Specification dialog box is displayed.

3. In the **Appliance** drop down list, select the appliance on which this job will run.

   Only those appliances previously defined for this system appear in this option list.

   If only one appliance is used for this system (the default), this field is automatically populated.

4. In the **Name** field, enter a name for this batch job.

5. From the **Type** drop down list, select **Global Action**.

   After you select the job type, additional options are displayed.

   - From the **Global Action** drop down list, select global action to perform. Only configured global actions will appear on the list.
   - From the **Off Global Action** drop down list, you have the option to select to a global action that is performed after the first global action expires.
   - From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.
6. Click **Next** to continue.
7. On the following page, select how often this batch job is run. From the **Repeat** drop down list, select one of the following options:

   - **Once** —- The batch job is run once. Click the **On** field to display the calendar and select a specific date and time.
   - **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter `30`.
   - **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.
   - **Weekly** — The batch job is run each week on the same day and time. Select the checkbox for each day the job will run, and enter the specific time in 24 hour format.
   - **Monthly** — The batch job is run each month on the same day and time. Select the days when the job will run and enter the specific time in 24 hour format. `Shift` + click to select a series of days, or `Ctrl` + click to select separate days.

   **Note:** If you selected an Off Global Action, you will have the option to enter when the Off action occurs. Otherwise, only the On field is displayed.

8. Click **Next**.

   A summary is displayed.
9. Click **Submit** to create this job.
10. To activate or deactivate this job, select the job and click **Activate/Deactivate**.

## Setting Batch Door Modes

Perform this procedure to change the door mode for a set of doors.

1. Select >**My Account** and click the Job Specification tab.
2. Click the **Add** button.

   The Job Specification dialog box is displayed.
3. In the **Appliance** drop down list, select the appliance on which this job will run.

   Only those appliances previously defined for this system appear in this option list.

   If only one appliance is used for this system (the default), this field is automatically populated.
4. In the **Name** field, enter a name for this batch job.

5. From the **Type** drop down list, select **Door Mode**.

   After you select the job type, additional options are displayed.

   - From the **Available** list, select the required doors then click ▶ to add it to the **Members** list.
   - From the **On Door mode** drop down list, select the door mode that you want to apply to the selected doors.
   - From the **Off Door mode** drop down list, select the door mode that you want to apply to the doors when the On action is complete.
   - From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.
   - Select the **Activate** checkbox to make the door modes active.
6. Click **Next** to continue.
7. On the following page, select how often this batch job is run. From the **Repeat** drop down list, select one of the following options:
   - **Once** —- The batch job is run once. Click the **On** field to display the calendar and select a specific date and time.
   - **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter `30`.
   - **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.
   - **Weekly** — The batch job is run each week on the same day and time. Select the checkbox for each day the job will run, and enter the specific time in 24 hour format.
   - **Monthly** — The batch job is run each month on the same day and time. Select the days when the job will run and enter the specific time in 24 hour format. `Shift` + click to select a series of days, or `Ctrl` + click to select separate days.

   **Note:** If you selected an Off Door Mode, you will have the option to enter when the Off action occurs. Otherwise, only the On field is displayed.

8. Click **Next**.

   A summary is displayed.
9. Click **Submit** to create this job.

# Permissions and Rights

The following table describes the permissions and rights the default Admin Role allows. All roles are made up of delegations. Each delegation is made up of rights.

| Permissions | Rights |
|---|---|
| View Events page | System Summary Listing |
| | System Summary Screen Refresh |
| | System Summary Get Layout |
| | System Summary Update Layout |
| | Monitor Listing |
| | Monitor Notes Show |
| | Monitor Instructions Show |
| | Monitor Identity Show |
| Search for events | Spork Listing |
| | Spork Search |
| | Monitor/Search Filters Save |
| | System Summary Get Layout |
| | System Summary Update Layout |
| View Alarms | Alarm Monitor Listing |
| | Monitor Notes Show |
| | Monitor Instructions Show |
| | Alarms Code Photo |
| | Monitor View Actions |
| | Maps-Alarms Show |
| Respond to alarm activity | Alarm Monitor Acknowledge |
| | Alarm Monitor Clear |
| | Alarms Create Notes |
| | Alarm Monitor Acknowledge All |
| | Alarm Monitor Clear All |
| | Alarm Monitor Identity |

| Permissions | Rights |
| --- | --- |
| View verifications | Swipe & Show |
| | Swipe & Show Get Doors |
| | Swipe & Show Get Door Name |
| | Get Photo |
| | Monitor Identity Show |
| | System Summary Get Layout |
| | System Summary Update Layout |
| View the status of assigned hardware | Monitor Listing |
| | Monitor Panels Status |
| | Monitor Periodic Update |
| | Monitor Appliance Status |
| Control assigned hardware | Doors Grant |
| | Doors Disable |
| | Doors Unlock |
| | Doors Lock |
| | Doors Restore |
| | Doors Mask Held |
| | Doors Mask Forced |
| | Doors Unmask Held |
| | Doors Unmask Forced |
| View and monitor status on assigned maps | Maps Monitor Listing |
| | Maps Show |
| | Maps Show Generate Image |
| | Maps Show Image |
| | Maps View Listing |
| | Maps Trace |
| | Mustering dashboard drill-down |

| Permissions | Rights |
| --- | --- |
| Control the assigned Bosch intrusion panels | Bosch Intrusion Area Clear Alarms |
| | Bosch Intrusion Area Disarm |
| | Bosch Intrusion Area Perimeter Delay Arm |
| | Bosch Intrusion Area Perimeter Force Delay Arm |
| | Bosch Intrusion Area Perimeter Force Instant Arm |
| | Bosch Intrusion Area Perimeter Instant Arm |
| | Bosch Intrusion Area Primary Delay Arm |
| | Bosch Intrusion Area Primary Force Delay Arm |
| | Bosch Intrusion Area Primary Force Instant Arm |
| | Bosch Intrusion Area Primary Instant Arm |
| | Bosch Intrusion Area Reset Sensors |
| | Bosch Intrusion Area Silence |
| | Bosch Intrusion Output Activate |
| | Bosch Intrusion Output Deactivate |
| | Bosch Intrusion Panel Command Execute |
| | Bosch Intrusion Panel Create |
| | Bosch Intrusion Panel Delete |
| | Bosch Intrusion Panel Detail Listing |
| | Bosch Intrusion Panel Detail Update |
| | Bosch Intrusion Panel Edit |
| | Bosch Intrusion Panel Listing |
| | Bosch Intrusion Panel Monitor Status |
| | Bosch Intrusion Panel Monitor Update |
| | Bosch Intrusion Panel New |
| | Bosch Intrusion Panel Update |
| | Bosch Intrusion Point Bypass |
| | Bosch Intrusion Point Unbypass |

| Permissions | Rights |
| --- | --- |
| Control the assigned DMP intrusion panels | DMP Intrusion Area Bypass Instant Arm |
| | DMP Intrusion Area Disarm |
| | DMP Intrusion Area Force Instant Arm |
| | DMP Intrusion Area Refuse Instant Arm |
| | DMP Intrusion Output Activate Momentary |
| | DMP Intrusion Output Activate Pulse |
| | DMP Intrusion Output Activate Steady |
| | DMP Intrusion Output Activate Temporal Code |
| | DMP Intrusion Output Deactivate |
| | DMP Intrusion Panel Command Execute |
| | DMP Intrusion Panel Config Update |
| | DMP Intrusion Panel Create |
| | DMP Intrusion Panel Delete |
| | DMP Intrusion Panel Detail Listing |
| | DMP Intrusion Panel Entities Update |
| | DMP Intrusion Panel Listing |
| | DMP Intrusion Panel Monitor Status |
| | DMP Intrusion Panel New |
| | DMP Intrusion Panel Reset Sensors |
| | DMP Intrusion Panel Show |
| | DMP Intrusion Panel Silence Alarm |
| | DMP Intrusion Zone Bypass |
| | DMP Intrusion Zone Unbypass |
| View live and recorded video | Cameras Show |
| | Cameras Login |
| | Monitor Cameras Show Video |

| Permissions | Rights |
| --- | --- |
| Add new identities. Cannot update fields after initial identity setup. | Identities My Account<br>Identities Listing<br>Identities Show<br>Identities Advance Search<br>Identities Date Search<br>Identity Profiles Listing<br>Identity Profiles Show List<br>Identities New<br>Identities Create<br>Identities Edit<br>Identity Profiles Populate Values<br>Identities Custom Layout Save |
| Force the identity to change the password at the next login to the ACM system. | Force Password Change |
| Add, modify, and update available roles | Identities Roles List<br>Identities Roles Update |
| Add, modify, and update tokens | Tokens Listing<br>Tokens Show<br>Tokens New<br>Tokens Create<br>Tokens Edit<br>Tokens Update<br>Tokens Set Free Pass<br>Identity Profiles Tokens Listing |
| Add and modify groups | Identities Groups List<br>Identities Groups Update |
| View assigned access permissions | Identities Show Access<br>Identity Profiles Show Access |
| Capture live photos and save | Identities Image Capture<br>Identities Image Save<br>Identities Code Image<br>Identities Photo Capture |

| Permissions | Rights |
| --- | --- |
| Add and upload photos | Identities Photo Edit<br>Identities Photo Update<br>Identities Photo Render<br>Identities Upload Photo |
| View transactional data | Identities Transactions |
| Print and issue badges | Identities Badge Show<br>Identities Badge Screen<br>Identities Print Badge<br>Identities Badge Render<br>Identities Update Badge Preview<br>Identities Update Badge |
| Perform REST actions | Identities Photo List REST<br>Identities Photo Show REST<br>Identities Photo Create REST<br>Identities Photo Update REST<br>Identities Photo Delete REST<br>Appliance REST Generation Transaction<br>REST Appliance Status Display<br>REST Get Doors<br>REST Get Identities<br>REST Get Identity<br>REST Get Inputs<br>REST Get Panels<br>REST Get Right Groups<br>REST Get Roles<br>REST Get Subpanels |
| REST call to list canned macros by the distinguished name (dn) of the door, input or output | Canned Macros Show |
| List canned macros by macro name | Canned Macros Listing |
| View Identity Policies | Identities Policies Show<br>Identities Policies Listing |

| Permissions | Rights |
| --- | --- |
| Add, modify, and delete Identity Policies | Identities Policies Create |
| | Identities Policies Edit |
| | Identities Policies New |
| | Identities Policies Update |
| | Identities Policies Delete |
| View reports | Reports Index |
| | Report Show |
| | Grant Access/Report |
| | Reports Show Grid |
| | Reports Custom Reports |
| Edit, preview, generate, and delete reports | Reports Edit |
| | Reports New |
| | Reports Create |
| | Reports Get Report Preview |
| | Reports Quick Report |
| | Reports Dynamic Criteria |
| | Reports Destroy |
| View Doors | Doors Listing |
| | Doors Show |
| | Interlocks Listing |
| | Doors Show Status |
| | Doors Effective Policy |
| | Doors Events List |
| | Doors Policy |
| | Access Levels Listing |
| | Access Levels Show |
| | Firmware Listing |
| | Macro Commands Listing |
| | Macro Commands Show |

| Permissions | Rights |
| --- | --- |
| View Panels | Panels Listing |
| | Panels Show |
| | Triggers Listing |
| | Panels Show Status |
| | Panel Effective Policy |
| | Panel Event List |
| | Firmware Apply View Log |
| View EOL Resistance | Resistance Levels Listing |
| View Areas | Areas Listing |
| | Areas Show |
| View Card Formats | Card Formats Listing |
| | Card Formats Show |

| Permissions | Rights |
| --- | --- |
| Add and modify Doors | ASSA ABLOY Doors Sync |
| | Doors New |
| | Doors Edit |
| | Doors Create |
| | Doors Update |
| | Doors New/Edit Appliance Change |
| | Doors New/Edit Manuf Change |
| | Doors Grant |
| | Interlocks New |
| | Interlocks Create |
| | Interlocks Edit |
| | Interlocks Update |
| | Interlocks Type Change New/Edit |
| | Interlocks Subpanel Change New/Edit |
| | Interlocks Trans Change New/Edit |
| | Interlocks Command Change New/Edit |
| | Interlocks Arg1 Change New/Edit |
| | Interlocks Arg2 Change New/Edit |
| | Interlock Trx Code Change New/Edit |
| | Doors Disable |
| | Doors Unlock |
| | Doors Lock |
| | Doors Download Status |
| | Doors - Download Parameters |
| | Doors - Reset |
| | Doors - Download Tokens |
| | Doors Restore |
| | Doors Mask Held |
| | Doors Mask Forced |
| | Interlocks with Type |
| | Doors Unmask Forced |
| | Doors Unmask Held |
| | Doors Cmacro Save |

| Permissions | Rights |
| --- | --- |
| | Doors Cmacro Type Change |
| | Doors Cmacro Op Type Change |
| | Doors Transactions |
| | Doors Assign Camera Type Change |
| | Doors Event Create |
| | Doors Event Edit |
| | Doors New/Edit Avail HW |
| | Doors Elevator I/O Naming |
| | Doors Edit - Panel Change |
| | Firmware New |
| | Firmware Create |
| | Firmware Apply |
| | Macro Commands New |
| | Macro Commands Edit |
| | Macro Commands Create |
| | Macro Commands Update |

| Permissions | Rights |
| --- | --- |
| Add and modify Panels | Panels New |
| | Panels Edit |
| | Panels Create |
| | Panels Update |
| | Panels Appliance Change New/Edit |
| | Panels Manf Change New/Edit |
| | Panels Status Details |
| | Panels Send Commands |
| | Panels Parameters Download |
| | Panels Tokens Download |
| | Panels Reset Download |
| | Triggers New |
| | Triggers Edit |
| | Triggers Create |
| | Triggers Update |
| | Triggers New/Edit Macro Change |
| | Triggers New/Edit Type Change |
| | Triggers New/Edit Subpanel Change |
| | Triggers New/Edit TrxType Change |
| | Triggers New/Edit Category Change |
| | Trigger New/Edit Trx Code Change |
| | Panel Rebuild Access Levels |
| | Panel Download Status |
| | Macro Commands Name Change |
| | Panels Model Change New/Edit |
| | Panels Set Free Pass |
| | Panels Event Create |
| | Panels Event Edit |
| Add and modify Areas | Area New |
| | Area Edit |
| | Area Create |
| | Area Update |

| Permissions | Rights |
| --- | --- |
| Add and modify EOL Resistance | Resistance Levels New |
| | Resistance Levels Edit |
| | Resistance Levels Create |
| | Resistance Levels Update |
| Add and modify Card Formats | Card Formats New |
| | Card Formats Edit |
| | Card Formats Create |
| | Card Formats Update |
| | Card Formats New/Edit Change Format |
| | Card Format Type Change |
| Delete hardware | Doors Delete |
| | Interlocks Delete |
| | Doors Cmacro Remove |
| | Doors Event Delete |
| | Firmware Delete |
| | Macro Commands Delete |
| | Panels Delete |
| | Triggers Delete |
| | Panel Events Delete |
| | Resistance Levels Delete |
| | Card Formats Delete |
| View Events | Events Listing |
| | Events Show |
| | Events Colors Listing |
| | Events Colors Show |
| | Subpanels Event List |
| | Inputs Event List |
| | Outputs Event List |
| | Event Logs Show |
| | Event Logs Listing |
| | Event Policies Show |
| | Event Policies Listing |

| Permissions | Rights |
| --- | --- |
| Edit Events | Events New |
| | Events Edit |
| | Events Create |
| | Events Update |
| | Event Colors New |
| | Event Colors Edit |
| | Event Colors Create |
| | Event Colors Update |
| | Subpanels Event Create |
| | Subpanels Event Edit |
| | Inputs Event Create |
| | Inputs Event Edit |
| | Outputs Event Create |
| | Outputs Event Edit |
| | Change Event Type |
| | Event Logs Create |
| | Event Logs Edit |
| | Event Logs New |
| | Event Logs Update |
| | Event Policies Create |
| | Event Policies New |
| | Event Policies Edit |
| | Event Policies Update |
| Delete Events | Events Delete |
| | Events Colors Delete |
| | Subpanels Event Delete |
| | Inputs Event Delete |
| | Outputs Event Delete |
| | Event Logs Delete |
| | Event Policies Delete |
| View Global Actions | Global Action Listing |
| | Global Action Show |

| Permissions | Rights |
| --- | --- |
| Edit Global Actions | Global Action New |
| | Global Action Edit |
| | Global Action Create |
| | Global Action Update |
| | Global Action Edit Type Change |
| | Global Action Execute |
| Delete Global Actions | Global Action Destroy |
| View Global Linkages | Global Linkage Listing |
| | Global Linkage Show |
| Edit Global Linkages | Global Linkage New |
| | Global Linkage Edit |
| | Global Linkage Create |
| | Global Linkage Update |
| | Global Linkage Edit Device Type |
| | Global Linkage Edit Token Search |
| | Global Linkage Edit Token Adv Search |
| | Global Linkage Remote Execute |
| Delete Global Linkages | Global Linkage Destroy |
| View Roles | Roles Listing |
| | Roles Show |
| | Roles Show Access |
| View Policies | Area Policies Listing |
| | Area Policies Show |
| | Area Policies Listing |
| | Area Policies Show |
| | Policies Listing |
| | Policies Show |
| View Groups | Groups Listing |
| | Groups Show |
| View Access Groups | Access Groups Listing |
| | Access Groups Show |
| | Access Group Show Access |

| Permissions | Rights |
| --- | --- |
| View Delegations | Delegations Listing |
| | Delegations Show |
| View Partitions | Partitions List |
| | Partitions Show |
| View Routing Groups | Routing Group Listing |
| | Routing Group Show |
| View Elevator Access Levels | Elevator Access Listing |
| Add and modify Roles | Roles New |
| | Roles Edit |
| | Roles Create |
| | Roles Update |
| | Roles Create Copy |
| | Roles Delete |
| | Roles Assign Delegation |
| | Roles Assign Groups |
| | Roles Assign Ports |
| | Roles Assign SO |
| Add and modify Policies | Area Policies New |
| | Area Policies Edit |
| | Area Policies Create |
| | Area Policies Update |
| | Door Policies New |
| | Door Policies Edit |
| | Door Policies Create |
| | Door Policies Update |
| | Policies New |
| | Policies Edit |
| | Policies Create |
| | Policies Update |

| Permissions | Rights |
| --- | --- |
| Add and modify Groups | Groups New |
| | Groups Edit |
| | Groups Create |
| | Groups Update |
| | Groups Member Assign |
| | Groups Policies Assign |
| | Groups/Identity Advanced Search |
| | Groups/Identity Advanced Criteria |
| Add and modify Access Groups | Access Groups New |
| | Access Groups Edit |
| | Access Groups Create |
| | Access Groups Create Copy |
| | Access Groups Update |
| | Access Groups Door Assign |
| Add and modify Delegations | Delegations New |
| | Delegations Edit |
| | Delegations Create |
| | Delegations Create Copy |
| | Delegations Delete |
| | Delegations Modify Members |
| Add and modify Routing Groups | Routing Group New |
| | Routing Group Edit |
| | Routing Group Create |
| | Routing Group Update |
| | Routing Group Update Groups |
| | Routing Group Update Types |
| Add and modify Elevator Access Levels | Elevator Access New |
| | Elevator Access Create |
| | Elevator Access Edit |
| | Elevator Access Update |

| Permissions | Rights |
| --- | --- |
| Delete Policies, Groups, Access Groups, Routing Groups, Elevator Access Levels | Area Policies Delete |
| | Door Policies Delete |
| | Policies Delete |
| | Groups Delete |
| | Access Groups Delete |
| | Routing Groups Delete |
| | Elevator Access Delete |
| View Appliance | Appliances Listing |
| | Appliances Show |
| | Appliance Ports Listing |
| | Serial Ports Listing |
| | Routes Listing |
| | Routes Show |
| | Appliance Software Listing |
| | Appliance Virtual Port List |
| | Appliance Software View Log |
| | Appliance Backup Listing |
| | Appliance Backup Show |
| | Appliance Status Display |
| | Appliance Log Download |
| | Appliance Log Show |
| | Appliance Backup Directory List |

| Permissions | Rights |
| --- | --- |
| Add and modify Appliances | Appliances New |
| | Appliances Edit |
| | Appliances Create |
| | Appliances Update |
| | Appliance Ports Edit |
| | Appliance Ports Update |
| | Serial Ports Edit |
| | Serial Ports Update |
| | Routes Edit |
| | Routes New |
| | Routes Create |
| | Routes Update |
| | Appliance Log |
| | Appliance Log Update |
| | Appliance Software New |
| | Appliance Software Create |
| | Appliance Software Apply |
| | Appliance Set System Date Time |
| | Appliance Backup Edit |
| | Appliance Backup Create |
| | Appliance Backup/Show Files |
| | Appliance Set Free Pass |
| | Appliance Show system Time |
| | Appliance Backup View Log |
| | Appliance Email Test |
| | Appliance Repl Subscription Add |
| | Appliance Repl Subscription Add (remote) |
| | Appliance Repl Subscription Remove (remote) |
| | Appliance Failover |
| | Appliance Failback |
| | Appliance Replication Update |
| | Appliance Replication Status |

| Permissions | Rights |
| --- | --- |
| | Run Backup Now |
| | Appliance Transaction Replication Status |
| | Appliance Backup Directory List, remote |
| | Appliance Backup Type USB |
| | Node Server Status Check |
| Delete Appliance | Appliances Delete |
| | Routes Delete |
| | Appliance Software Delete |
| View System Setup | Schedules Listing |
| | Schedules Show |
| | Holidays Listing |
| | Holidays Show |
| | Event Types Listing |
| | Event Types Show |
| | Get Event Types for Device |
| | Get Alarm Types for Device |
| Add and modify System Setup | Schedules New |
| | Schedules Edit |
| | Schedules Create |
| | Schedules Update |
| | Holidays New |
| | Holidays Edit |
| | Holidays Create |
| | Holidays Update |
| | Event Types New |
| | Event Types Edit |
| | Event Types Create |
| | Event Types Update |
| Delete System Setup | Schedules Delete |
| | Holidays Delete |
| | Event Types Delete |

| Permissions | Rights |
| --- | --- |
| View User Fields and User Lists | User Defined Tabs Listing |
| | User Defined Tabs Show |
| | User Defined Fields Listing |
| | User Defined Fields Show |
| | User Lists Index |
| Add and modify User Fields and User Lists | User Defined Tabs New |
| | User Defined Tabs Edit |
| | User Defined Tabs Create |
| | User Defined Tabs Update |
| | User Defined Tabs Edit/Assign |
| | User Defined Fields New |
| | User Defined Fields Edit |
| | User Defined Fields Create |
| | User Defined Fields Update |
| | User Lists Edit |
| | User Lists Update |
| Delete User Fields and User Lists | User Defined Tabs Delete |
| | User Defined Tabs Delete |
| View System Settings | External Domains Show |
| | External Domains Index |
| | System Settings Index |
| Add and modify System Settings | System Settings Update |
| | System Settings Edit |
| | External Domains Update |
| | External Domains Edit |
| | External Domains New |
| | External Domains Create |
| | External Domains List Certificates |
| | External Domains Create Certificates |
| | External Domains Load Certificates |
| | System Settings Edit (in place) |
| | System Settings Enhanced Access Level |

| Permissions | Rights |
| --- | --- |
| Delete System Settings | External Domains Destroy |
| | External Domains Destroy Certificates |
| View Badge Designer | Badge Templates Listing |
| | Badge Templates Show |
| Add and modify badge templates in the Badge Designer | Badge Templates New |
| | Badge Templates Edit |
| | Badge Templates Create |
| | Badge Templates Update |
| | Badge Templates Generate Image |
| | Badge Templates Add Details |
| | Badge Template Copy |
| | Badge Template Preview |
| Delete badge templates in the Badge Designer | Badge Templates Delete |
| View External Systems | Image Devices Listing |
| | Image Devices Show |
| | Exacq Server List |
| | Exacq Show |
| | External Systems Listing |
| | External Systems Show |
| | Avigilon Show |
| | Avigilon Server List |
| | Salient Server List |
| | Salient Server Show |
| | Salient Cameras List |
| | Milestone Server List |
| | Milestone Server Show |
| | Avigilon Server Camera List |
| | Avigilon Server Status |
| | Intrusion Panel Listing |
| | Intrusion Panel Show |
| | Intrusion Panel Detail Listing |

| Permissions | Rights |
| --- | --- |
| Add and modify External Systems | Image Devices New |
| | Image Devices Edit |
| | Image Devices Create |
| | Image Devices Update |
| | Exacq Server Create |
| | Exacq Server Edit |
| | Exacq Server New |
| | Exacq Update |
| | External Systems Edit |
| | External Systems Update |
| | External Systems New |
| | External Systems Create |
| | Avigilon Server Create |
| | Avigilon Server Edit |
| | Avigilon Server New |
| | Avigilon Update |
| | Salient Server New |
| | Salient Server Create |
| | Salient Server Edit |
| | Salient Server Update |
| | Salient Cameras PTZ Control |
| | Milestone Server New |
| | Milestone Server Edit |
| | Milestone Server Create |
| | Milestone Server Update |
| | Avigilon Server Cameras |
| | Avigilon Server Add/Update Cameras |
| | HID Origo Connection Create |
| | HID Origo Connection Delete |
| | HID Origo Connection Listing |
| | HID Origo Connection Send Invitation |
| | HID Origo Connection Update |
| | Intrusion Panel New |

| Permissions | Rights |
| --- | --- |
| | Intrusion Panel Create |
| | Intrusion Panel Edit |
| | Intrusion Panel Update |
| | Intrusion Panel Detail Update |
| | SALTO Server Create |
| | SALTO Server Listing |
| | SALTO Server Update |
| | Virdi Biometric Create |
| | Virdi Biometric Listing |
| | Virdi Biometric Update |
| Delete External Systems | Image Devices Delete |
| | Exacq Server Delete |
| | External Systems Delete |
| | Avigilon Server Remove |
| | Salient Server Delete |
| | Milestone Server Delete |
| | SALTO Server Delete |
| | Virdi Biometric Delete |
| *Mercury Security panels only*<br>Add, modify and delete custom certificates | Certificates Create |
| | Certificates Destroy |
| | Certificates Edit |
| | Certificates Listing |
| | Certificates New |
| | Certificates Show |
| | Certificates Update |
| View Maps | Maps Listing |
| | Maps Show |
| Add and modify Maps | Maps New |
| | Maps Edit |
| | Maps Create |
| | Maps Update |
| | Maps Edit and Add Detail |

| Permissions | Rights |
| --- | --- |
| Delete Maps | Maps Delete |
| View Collaboration | Collaboration Listing |
| | Collaboration Show |
| Edit Collaboration | Collaboration New |
| | Collaboration Edit |
| | Collaboration Create |
| | Collaboration Update |
| | Collaboration Type Change New/Edit |
| | Collaboration Assign Event Types |
| | Collaboration Connection Test |
| | Collaboration Table Change |
| | Collaboration Database Search |
| | Collaboration Edit (gw-change) |
| | Collaboration Identity Write/Logs |
| | Collaboration Identity Read/Logs |
| | Identity Collabs Preview |
| | Collaboration CSV Recurring, Directory List |
| | Collaboration CSV Recurring, remote |
| Delete Collaboration | Collaboration Delete |
| View account details, batch jobs, and job specifications | Identities MyAccount |
| | Batch Job Specification Index |
| | Batch Job Specification New |
| | Batch Job Index |
| | View Batch Update Schedules |

| Permissions | Rights |
| --- | --- |
| Create, edit, and delete batch jobs and job specifications | Batch Job Specification Edit<br>Batch Job Specification Activate<br>Batch Job Specification PostProcess<br>Batch Job Specification JobSpecificationList<br>Batch Job Specification Create<br>Batch Job Specification Update<br>Batch Job Create<br>Batch Job New<br>Batch Job Update<br>Batch Job List<br>Batch Job Output<br>Custom Report Schedule<br>Reset Custom UI Settings<br>System Settings Localize<br>Batch Job Specification Destroy<br>Batch Job Destroy |

## Permissions and Rights for MFA

| Permissions | Rights |
| --- | --- |
| Add and delete MFA devices to support two-step identity authentication when logging in to the ACM application | MFA Device Add<br>MFA Device Remove |

# Permissions and Rights for Sound Assets

| Permissions | Rights |
| --- | --- |
| Add, delete, update, save, and view sound assets in the ACM application | Sound Asset Create |
| | Sound Asset Delete |
| | Sound Asset Edit |
| | Sound Asset Listing |
| | Sound Asset New |
| | Sound Asset Preview |
| | Sound Asset Update |

# Permissions and Rights for ACM Expedite Mobile App Users

Ensure the following rights are assigned to a role in the ACM application for mobile app users. For more information about the mobile app, see the ACM *Expedite Mobile App User Guide*.

| Permissions | Rights |
|---|---|
| View doors in the mobile app, including lists and details | Doors Listing<br>Doors Show |
| Issue global actions in the mobile app | Global Action Execute |
| View global actions in the mobile app, including lists and details | Global Action Listing<br>Global Action Show |
| View identities in the mobile app, including lists and details | Identities Listing<br>Identities Show<br>Identity Group List<br>Identity Role List<br>Identity Update |
| Update tokens on the identity page in the mobile app, including status | Token Listing<br>Token Status Update<br>Token Update |

# Troubleshooting

## Events

To view events, do one of the following:

- Select **Monitor** > **Events** and search for events.
- Select **Physical Access** > **Doors**, the door name and then the **Transactions** tab.

**Note:** The default event names and event types in this section may be customized in your ACM application. For more information, see *Customizing ACM System Events* on page 312.

### Appliance Events

Source Type: Appliance

| Event | Description |
|---|---|
| *System* | |
| CPU Load High | The five-minute CPU load average across all threads is running at a high level. |
| CPU Load Normal | The five-minute CPU load average across all threads is running at a low-to-medium level. |
| Database Disk Space Low | Less than 10% (inclusive) of free disk space is available in the database disk partition. |
| Database Disk Space Normal | More than 10% of free disk space is available in the database disk partition. |
| Network Port 1 Link Down | The link is down for network port-1 on the appliance. |
| Network Port 1 Link Normal | The link is up for network port-1 on the appliance. |
| Network Port 2 Link Down | The link is down for network port-2 on the appliance. |
| Network Port 2 Link Normal | The link is up for network port-2 on the appliance. |
| Programs Disk Space Low | Less than 5% (inclusive) of free disk space is available in the programs disk partition. |
| Programs Disk Space Normal | More than 5% of free disk space is available in the programs disk partition. |
| System Memory Low | Less than 10% (inclusive) of system memory (RAM) is available on the appliance. |
| System Memory Normal | More than 10% of system memory (RAM) is available on the appliance. |

### Door Events

When a door is not operating as expected, review the event transactions.

**Note:** The event transactions depend on events that are sent from locks and devices over various technologies. Allow time for the events to appear in the ACM application.

Source Type: Door

ASSA ABLOY IP-enabled doors refer to hard-powered PoE (Power over Ethernet) locks and battery-powered Wi-Fi locks.

SALTO doors refer to online and standalone (offline) doors.

| Event | Description | Device |
|---|---|---|
| *Communications* | | |
| Door service was offline before system audit | The audit buffer got full before audits could be retrieved from the lock. | Control locks, LE, LEB, NDE, NDEB, RM, RU |
| Out of Sync | The door is out of sync with the DSR and ACM system. | ASSA ABLOY IP-enabled doors |
| RF loss / Lock offline | Any of:<br>• Communication to the linked device over radio frequency was disconnected.<br>• Lock is offline. | Control locks, LE, LEB, LE (RSI mode), NDE, NDEB, RM, RU |
| | | |
| *Door held open* | | |
| Door held masked | A door held masked event occurred. | ASSA ABLOY IP-enabled doors |
| Door held open | A door held open event occurred. | ASSA ABLOY IP-enabled doors and Schlage AD-400, LE, LEB, LE (RSI mode), NDE, NDEB, RM, RU |
| Door held unmasked | A door held unmasked event occurred. | ASSA ABLOY IP-enabled doors |
| *Forced Door* | | |
| Forced door | A forced door event occurred. | ASSA ABLOY IP-enabled doors and Schlage AD-400, LE, LEB, LE (RSI mode), NDE, NDEB, RM, RU |
| Forced door masked | A forced door masked event occurred. | ASSA ABLOY IP-enabled doors |
| Forced door unmasked | A forced door unmasked event occurred. | ASSA ABLOY IP-enabled doors |
| *Invalid Credential* | | |

| Event | Description | Device |
|---|---|---|
| Attempt to open Locked Door | Access was attempted when the door mode was set to Locked No Access. | ASSA ABLOY IP-enabled doors |
| Duress Detected - Access Denied | A duress code was detected at the door, and therefore, access was denied. | Mercury doors with PIN keypad |
| Expired Card Attempt | No access granted when an expired token was swiped at the reader.<br><br>*For LE, LEB, NDE and NDEB locks.* In the Deactivate Date field, the token expires at the start of the specified hour. For example, if 17:00:00 is specified, the token expires at 16:00:00.<br><br>*For ASSA ABLOY IP-enabled and Control locks.* In the Deactivate Date field, the token expires at the start of the specified minute and second. For example, if 17:10:10 is specified, the token expires at 17:10:00.<br><br>To resolve this issue, do any of:<br><br>• Set the Deactivate Date to the next date.<br>• Set the Deactivate Date to the same date and next hour (for LE, LEB, NDE and NDEB), or next minute and second (Control). | ASSA ABLOY IP-enabled doors, Control locks, LE, LEB, NDE, NDEB |
| Invalid Card - Before Activation | An invalid card was detected before its activation. | Schlage AD-400 and LE (RSI mode) |
| Invalid card format | An invalid card format occurred. | Schlage AD-400 and LE (RSI mode) |
| Invalid Card Schedule | Access was attempted outside of the allowed date and timed access for the identity. | Any door |
| Unknown card | The swiped card is not known to the door because the token was not downloaded. | ASSA ABLOY IP-enabled doors and Schlage AD-400 and LE (RSI mode) |
| Invalid PIN code has been entered | The card was not granted access to the door due to an invalid PIN code. | Any door |
| Valid card at an unauthorized reader | A valid card was presented at an unauthorized reader. | Schlage AD-400 and LE (RSI mode) |
| *Maintenance* | | |
| Door has been restored | The door mode or custom mode has been restored. | SALTO online door |
| Incompatible Firmware Image | A user attempted to update a lock with an incompatible firmware image. | Schlage IP-enabled locks |

| Event | Description | Device |
|---|---|---|
| Magnetic Tamper | A magnetic tamper event occurred. | LE, LEB, NDE, NDEB, RU, RM |
| Token capacity exceeded | A token cannot be added due to the lock capacity. | ASSA ABLOY IP-enabled doors, Schlage ENGAGE locks |
| *System* | | |
| Deadbolt | A deadbolt was used. | Schlage AD-400 |
| Door has been added | *For Offline Wi-Fi locks*. The lock on the door has been externally commissioned through the ENGAGE gateway application. | LE, LEB, NDEB |
| Door has been locked | The door has been locked. | Any door |
| Door has been unlocked | The door has been unlocked. | Any door |
| Door in card only mode | A door in Card Only mode was detected. | Schlage AD-400 and LE (RSI mode) |
| Door opened | The door is open. | ASSA ABLOY IP, Mercury Security, HID and Schlage IP-enabled doors |
| Escape and Return Unlock Active | The Escape and Return mode is active (Exit Leaves Open or Toggle and Exit Leaves Open door mode). | SALTO doors with no control unit |
| Escape and Return Unlock Inactive | The Escape and Return mode is inactive (Exit Leaves Open or Toggle and Exit Leaves Open door mode). | SALTO doors with no control unit |
| Host Rex, Door not used | A request to exit was initiated but the door was not used. | Schlage AD-400 |
| Host Rex, Door used | A request to exit was initiated and the door was used. | Schlage AD-400 |
| Host Rex, Non-verified | A request to exit was initiated (non-verified). | Schlage AD-400 |
| Host Rex, Use Pending | A request to exit was initiated and door use is pending. | Schlage AD-400 |
| Motor Stall | A motor stall occurred. | Schlage AD-400 |
| Rex Pressed, Door used | The door handle was used. | ASSA ABLOY IP, Mercury Security, HID, SALTO and Schlage IP-enabled doors; LE (RSI mode) |
| *Tamper* | | |

| Event | Description | Device |
|---|---|---|
| Bezel Tamper | A bezel tamper occurred. | Schlage AD-400 and LE (RSI mode) |
| Bluetooth Tamper - Door | A Bluetooth configuration device was connected to the door, which caused the door to disconnect from the gateway.<br>To resolve this issue:<br>• Disconnect the configuration device. | Control locks, LEB, NDEB, RM, RU |
| Keyswitch | A physical key was used to access the door. | ASSA ABLOY IP-enabled and Schlage AD-400 |
| Reader/Device Tamper | A tamper event occurred in any of:<br>• The reader or linked device.<br>• The cover of the crash bar or push bar. | Control locks, LEB, NDEB, RM, RU |
| *User audit* | | |
| Door grant request | A door grant request was initiated. | Schlage AD-400 and LE (RSI mode) |
| *Valid Credential* | | |
| Keypad Code Grant | The correct access code was entered at the door that is configured for Keypad Only door mode.<br>**Note:** No event is logged when an incorrect keypad code is entered at the door. | SALTO online doors |
| Invalid key | The access code on the key is no longer valid. | SALTO online doors |
| Local Grant | Access was granted to an identity that has access to the door and has swiped the card. | Any door |
| Local Grant - Duress - Not Used | Access was granted to an identity that has access to the door and has not entered a duress keypad code or duress PIN during a security situation. | Mercury doors with PIN keypad |
| Local Grant - Duress - Used | Access was granted to an identity that has access to the door and has entered a duress keypad code or a duress PIN during a security situation. | Mercury doors with PIN keypad, SALTO online doors |

## Battery Level Events

Source Type: Door

| Event | Description | Device |
|---|---|---|
| Door Critical Battery | The battery is running critically low. | All battery-powered locks except for SimonsVoss wireless locks |
| Door low battery | The battery is running low. | |
| NORMAL Door Critical Battery | The battery is no longer running critically low. | |
| NORMAL Door low battery | The battery is no longer running low. | |

## Control Lock Events

IP-connected doors only

Source Type: Door

| Event | Description | Device |
|---|---|---|
| *System* | | |
| Deadbolt | Any of:<br>• The deadbolt was locked (extended) after a Local Grant event.<br>• Deadbolt usage. | Control locks |
| NORMAL - Deadbolt | Any of:<br>• The deadbolt was unlocked (retracted) after a Local Grant event.<br>• Deadbolt usage. | Control locks |

## RU and RM Device Events

IP- and RSI-connected doors only

Source Type: Door

| Event | Description | Device |
|---|---|---|
| *Communications* | | |
| DPS communication failure | A DPOS communication failure has occurred. | RU, RM |
| *Maintenance* | | |
| Dogging mechanism failure | The latch hook in the push bar did not release and requires intervention by personnel to unlock the door. | RU |
| Latch mechanism failure | The latch bolt did not retract during exit and requires intervention by personnel. | RU, RM |
| *System* | | |
| Unlock on next exit request | The ACM system sent an Unlock on next exit request to the door. | RU |
| *Tamper* | | |

| Event | Description | Device |
|---|---|---|
| Door has been locked manually | The door in DNE state was locked by personnel using the hex key. | RU, RM |
| Door has been unlocked manually | The door was unlocked by personnel using the hex key and pressing the push bar. | RU, RM |
| Door security compromised | The latch in the push bar was not extended due to tampering of the closed door. | RU, RM |
| Unlock on next exit (manual) | The latch in the push bar was retracted by personnel using the hex key, which sets up the door to be unlocked by the next person who presses the push bar. | RU, RM |

# Intrusion Events

## DMP Intrusion Events

Source Type: DMP Intrusion Area, DMP Intrusion Output, DMP Intrusion Panel, DMP Intrusion User, DMP Intrusion Zone

**Note:** Some events are dependent on DMP firmware versions.

### *DMP Intrusion Area*

Source Type: DMP Intrusion Area

| Event | Description |
|---|---|
| DMP Area armed | The area was armed. |
| DMP Area armed (All areas armed) | All areas in the system were armed. |
| DMP Area disarmed | The area was disarmed. |
| DMP Late to arm | The area was armed outside of the schedule assigned to the area. |

### *DMP Intrusion Output*

Source Type: DMP Intrusion Output

| Event | Description |
|---|---|
| - | - |

### *DMP Intrusion Panel*

Source Type: DMP Intrusion Panel

| Event | Description |
|---|---|
| Event Type: Intrusion DMP | |
| DMP * * AMBUSH * * | A silent alarm was initiated by a user during an emergency situation. |

| Event | Description |
|---|---|
| DMP A.C. power restored | The A.C. power was restored to the panel. |
| DMP ALERT: System recently armed | An alarm message was generated within five minutes of the panel being armed. Informs the central station that the panel was armed before the alarm occurred. |
| DMP ALERT: Unauthorized Entry | An area was disarmed by a user outside of their scheduled access time. Access setup is dependent on the hardware model.<br><br>**Note:** To resolve this event, do any of the following:<br>• Add a schedule to the profile.<br>• Delete all access schedules from the profile.<br>• Add an access area to a profile that is in a schedule.<br>• Change one of the assigned schedules. |
| DMP Automatic recall test OK | The panel is communicating as expected in an automatic communication test. |
| DMP Communication line level restored | The panel detected that communication to the cellular tower was restored. |
| DMP Late to Close | The system was not armed at its scheduled closing time. |
| DMP Lockdown cleared | A lockdown was cleared, either using the keypad by a DMP user or remotely by a Remote LInk user. |
| DMP Lockdown initiated | A lockdown was issued in an emergency situation to lock all doors designated as public, either using the keypad by a DMP user or remotely by a Remote Link user. |
| DMP Panel Restart | The panel was restarted. |
| DMP Receiver EEPROM Error | The panel detected an Electronically Erasable Programmable Read Only Memory (EEPROM) error in equipment, such as a printer or line card. |
| DMP Service Code Start | A service authorization code was entered by service personnel before accessing panel operations or programming. An authenticated code can be used for 30 minutes before requiring authentication again. |
| DMP Service Code Stop | The service authorization code must be authenticated again (30 minutes have elapsed). |
| DMP Standby battery restored | The panel battery voltage was restored to greater than 12.6 VDC at the last battery test. |
| DMP TROUBLE OVERRIDE | A system trouble message was acknowledged by a DMP user who selected OKAY when arming the system. |
| DMP Telephone line 1 restored | The panel detected that its main telephone connection is operational. |

| Event | Description |
|---|---|
| DMP Telephone line 2 restored | The panel detected that the second telephone line is operational. |
| DMP WARNING: A.C. power failure | The main A.C. power is not present or is less than 85% of the expected voltage. The warning is sent after the expiration of the panel programmed delay time. |
| DMP WARNING: Alarm bell silenced | The panel's main bell circuit was silenced by a code entry at a panel keypad. |
| DMP WARNING: Low communication line level | The panel detected that communication to the cellular tower was missing for more than 180 seconds. |
| DMP WARNING: Low standby battery | The standby battery fell below 11.9 VDC. The battery is tested at 15 minutes past each hour. |
| DMP WARNING: Telephone line 1 trouble | The panel detected that its main telephone connection is disconnected or is non-operational. |
| DMP WARNING: Telephone line 2 trouble | The panel detected that the second telephone connection is disconnected or is non-operational. |
| Event Type: User audit | |
| Intrusion Panel Command Request | A request was generated in the ACM application to update the intrusion panel, area, zone or output configuration. |
| Other supported events: | |
| DMP ContactID, DMP Equipment Added, DMP Equipment Adjusted, DMP Equipment Removed, DMP Equipment Repaired, DMP Equipment Replaced, DMP Equipment Test | |

### *DMP Intrusion User*

Source Type: DMP Intrusion User

| Event | Description |
|---|---|
| DMP Access denied - anti-passback | Door access in an anti-passback area was denied to a user (an identity in ACM) who did not use the proper door to exit an area they had previously accessed. |
| DMP Access denied - armed area | Door access to an armed area was denied to a user (an identity in ACM). |
| DMP Access denied - inactive user | Door access was denied to an inactive user (an identity in ACM). |
| DMP Access denied - invalid area | Door access was denied to a user (an identity in ACM) trying to access an area that is not assigned to their user code or profile. |
| DMP Access denied - invalid code | Door access was denied to a user (an identity in ACM) using an invalid user code, or if the two man (person) rule configuration is enabled, the second code was not entered or the same code was entered twice. |
| DMP Access denied - invalid time | Door access was denied to a user (an identity in ACM) trying to access an area at a time that is outside all schedules in all profiles assigned to the user. |

| Event | Description |
|---|---|
| DMP Access denied - invalid user level/profile | Door access was denied to a user (an identity in ACM) trying to access a door that is not enabled in any profile assigned to the user. |
| DMP Door access | Door access was provided to a user (an identity in ACM). |
| DMP Holiday A change | A holiday date, type A, was changed by a DMP user. |
| DMP Holiday B change | A holiday date, type B, was changed by a DMP user. |
| DMP Holiday C change | A holiday date, type C, was changed by a DMP user. |
| DMP Holiday change | A holiday date was changed by a DMP user. |
| DMP Permanent schedule change | A permanent schedule was changed by a DMP user. |
| DMP Primary schedule change | A primary schedule was changed by a DMP user. |
| DMP Secondary schedule change | A secondary schedule was changed by a DMP user. |
| DMP Shift 1 schedule change | A shift schedule was changed by a DMP user. |
| DMP Shift 2 schedule change | A shift schedule was changed by a DMP user. |
| DMP Shift 3 schedule change | A shift schedule was changed by a DMP user. |
| DMP Shift 4 schedule change | A shift schedule was changed by a DMP user. |
| DMP User code added | A user code was added by a DMP user. |
| DMP User code changed | A user code was changed by a DMP user. |
| DMP User code deleted | A user code was deleted by a DMP user. |
| DMP User code inactive | For XR550 only. A user code expired after a period of inactivity. |

### *DMP Intrusion Zone*

Source Type: DMP Intrusion Zone

| Event | Description |
|---|---|
| DMP Dirty smoke detector | A 'dirty smoke detector' service message was sent for the zone. |
| DMP Zone alarm | A burgulary, carbon monoxide, fire, or generic alarm occurred in a zone (for example, east warehouse). |
| DMP Zone bypassed | A zone was bypassed by the DMP user. |
| DMP Zone failed | A 'zone failed' message was sent for the zone. |
| DMP Zone faulted | A 'zone faulted' message was sent for the zone. |
| DMP Zone force armed | A 'zone force armed' message was sent for the zone. |
| DMP Zone low battery | A 'low battery' message was sent for the zone. |
| DMP Zone missing | A 'zone missing' message was sent for the zone. |

| Event | Description |
|---|---|
| DMP Zone reset | A zone was reset. |
| DMP Zone restored | A zone was restored to the expected condition from a bad condition. |
| DMP Zone tamper | A 'zone tamper' message was sent for the zone (for example, a wireless keypad tamper). |
| DMP Zone trip count | The number of zone trips was sent for the zone. |
| DMP Zone trouble | A 'zone trouble' message was sent for the zone (for example, a wireless keypad tamper). |
| DMP Zone verified | A 'zone verify' message was sent for the zone. |

## Panel Events

Source Type: Panel

| Event | Description | Device |
|---|---|---|
| *Communications* | | |
| Panel offline | The panel is offline. | Mercury Security panel, SALTO server, Schalge ENGAGE gateway (RSI mode) |
| *Maintenance* | | |
| Maximum panel schedule count exceeded | The maximum number of schedules configured for a panel has been exceeded.<br><br>For Mercury Security and ASSA ABLOY IP-enabled doors, the limit is 255 schedules. For Schlage IP/PoE mode doors, the limit is 16 intervals in all schedules combined. For SALTO doors, the limit is 1024 schedules.<br><br>To resolve this issue, do any of the following:<br>• Assign fewer schedules to the panel.<br>• Identify unneeded schedules on the Schedules tab on the panel page.<br>• Move hardware to a different or new panel. | ASSA ABLOY DSR, Mercury Security panel, SALTO server, Schlage ENGAGE gateway (IP and RSI mode) |
| Panel Firmware Download Started | A panel firmware download request has started in the ACM application. | Mercury Security panel |
| Panel Full Parameter Download Started | A panel parameter download request has started in the ACM application. | Mercury Security panel |
| Panel Full Token Download Started | A panel token download request has started in the ACM application. | SALTO server |
| Panel sync request completed | A panel sync request has completed in the ACM application. | SALTO server |

| Event | Description | Device |
|---|---|---|
| Panel sync request started | A panel sync request has started (and not completed yet) in the ACM application. | SALTO server |
| *Tamper* | | |
| Panel transaction limit reached | The maximum number of transactions configured for the subpanel was reached. | Mercury Security panel |

## SALTO Key Events

Source Type: Credentials

| Event | Description | Device |
|---|---|---|
| *User Audit* | | |
| Key Assignment completed | A key was assigned to a token in the ACM system. | SALTO doors |
| Key Assignment started | A key assignment to a token was started in the ACM system. | SALTO doors |
| Key Cancelled | A key was cancelled in the ACM system. | SALTO doors |
| Key Update completed | A key update was completed in the ACM system. | SALTO doors |
| Key Update started | A key update was started in the ACM system. | SALTO doors |

## Subpanel Events

Source Type: Subpanels

| Event | Description | Device |
|---|---|---|
| *Communications* | | |
| Subpanel offline | The subpanel is offline. | Schalge ENGAGE gateway subpanel (RSI mode) |

## System Events

Source Type: System

| Event | Description |
|---|---|
| CSR Created | An SSL certificate signing request (CSR) was created in the ACM application. |
| Expired Transactions Removed | The expired transactions were removed from the appliance when the threshold was reached. For more information, see the Max Days Stored setting. |
| New Cert Generated | A new SSL certificate was generated in the ACM application. |
| New Cert Taken Into Use | A new SSL certificate was applied to the appliance. |
| New Cert Uploaded - Failure | The new SSL certificate was not uploaded to the appliance. |

| Event | Description |
|---|---|
| New Cert Uploaded - Success | The new SSL certificate was uploaded to the appliance. |
| Transaction log exceeded 85% | The transactions stored in the appliance have exceeded 85% of the maximum stored transactions threshold.* |
| Transaction log exceeded 95% | The transactions stored in the appliance have exceeded 95% of the maximum stored transactions threshold.* |
| Transaction log exceeded threshold | The transactions stored in the appliance were purged. For more information, see the Max Stored Transactions setting.* |

* See also *Appliance Transactions Indicators* on page 43.

# Enabling Debug Logs

**Note:** Enabling the appliance logs requires these delegations: Appliance Log, Appliance Log Download, Appliance Log Show, and Appliance Log Update. Contact your support representative to enable the Debug checkbox, if needed.

To debug using the appliance logs:

1. Select > **Appliance** and the **Access** tab.
2. Put a checkmark in the **Debug** checkbox next to the vendor.
3. Click .

See also *Accessing Appliance Logs* on page 353.

# Appendix: pivCLASS Configuration

**Note:** Refer to this information only if you are installing ACM and are required to use the Federal Information Processing Standard (FIPS) 140-2 certified cryptographic module and pivCLASS solution for FIPS 201-2 certified sites.

## Overview

This section is intended for ACM operators who are using the pivCLASS application, authentication module (PAM) and pivCLASS readers to validate the authenticity of Personal Identification Verification (PIV) and PIV-Interoperable (PIV-I) cards. The NIST cryptographic functionality enables ACM™ system to comply with FIPS 140-2 requirements.

The FIPS-certified crytographic module and pivCLASS readers are supported on all ACM platforms.

## Prerequisites

Partners who install the pivCLASS application, authentication module (PAM) and pivCLASS readers are recommended to take pivCLASS software and public key infrastructure (PKI) at the door certification training. For more information, see Genuine HID Academy Learning Center.

## Enabling FIPS 140-2 Encryption on ACM Appliances

Follow these steps if:

- If you are required to use ciphers that are certified as compliant with the Federal Information Processing Standard (FIPS) Publication 140-2 (a U.S. government computer security standard used to approve cryptographic modules, titled "Security Requirements for Cryptographic Modules").
- If you are using only door controllers that support the cryptographic module certified by the U.S. government with the ACM system. For our compliance certificate, see National Institute of Standards and Technology (NIST) certificate #4588. Only Mercury LP-series controllers support this cryptographic module.

To enable FIPS 140-2 encryption on an ACM appliance:

1. On the **Appliance** page, select the **Use FIPS 140-2 compliant ciphers only** checkbox.

   This setting is system-wide and triggers an automatic restart of the ACM appliance when it is selected.

   When this checkbox is:

   - Not Enabled (the default) — A cipher that is not FIPS compliant is used to encrypt traffic in the ACM system.
   - Enabled — The ACM system only uses FIPS 140-2 compiant ciphers.

   A warning message is displayed.
2. Click **OK** to confirm.

The ACM appliance is restarted, and now the ACM system is using the FIPS 140-2 encryption. No additional steps are required to configure Mercury panels.

# Enabling Large Encoded Card Format and Embedded Authorization on Panels

Use the following fields when you add a panel to the ACM system, depending on the type of authentication in use at your site.

| Authentication Subsystem | Enable Large Encoded Card Format | Embedded Auth |
|---|---|---|
| None | (uncheck) | None |
| pivCLASS with external PAM | (check) | None |
| pivCLASS embedded AAM for Mercury LP4502 only | (check) | pivCLASS |

On the Panel: Add page:

- For Mercury LP4502 model only. In the **Embedded Auth** field, select **pivCLASS**. The Enable Large Encoded Card Format field is automatically selected.
- For all other types of Mercury controllers. Select the **Enable Large Encoded Card Format** field (non-reversible; see Note below):
  - Used for internal numbers that are larger than 64 bits. For example, 128-bit and 200-bit cards need the 32-character Federal Agency Smart Credential Number (FASC-N) or Card Holder Unique Identifier (CHUID) for PIV-I cards. Large Encoded card formats are used with FIPS 201 certified pivCLASS readers; see Approved Product List (APL) #10122.
  - Used typically to enable authentication by pivCLASS readers at FIPS 201-2 certified sites.

**Note:** The panel cannot be reconfigured after this setting is selected. To accept any other card format other than large formats, delete it and re-add it to the ACM system.

# Updating Firmware

To update the firmware of the Mercury LP4502 panel:

1. On the Panels  list, select the panel and then on the Status tab, click **Firmware**.
2. To add support for the authentication module on the panel, install the **pivCLASS-Embedded-Auth_Pkg_05_10_27_#145.crc** firmware version.

   To remove the authentication module from the panel, install the **pivCLASS-Embedded-Auth-Removal_Pkg_01_00_00_#14.crc** firmware version.
3. To verify the installation of the firmware, review the panel status page which shows the name and version of the pivCLASS package along with the authentication module and firmware versions.
4. For pivCLASS embedded AAM for Mercury LP4502 only. After the firmware is installed, you must configure communication between the panel and pivCLASS service. For more information about configuring the pivCLASS-Embedded-Auth fields on the Configuration Manager for the panel, refer to Mercury documentation.

# Adding Doors

When adding a door with pivCLASS embedded AAM for the Mercury LP4502 model, do the following:

- Ensure the **Name** field is updated as follows. If your site uses pivCLASS-compliant credentials to authenticate credentials, the **Name** of the door that you enter in the ACM system must match the reader name entered in the Description field of the reader in the pivCLASS registration system. Before adding doors, ensure you that you know the reader name entered in the pivCLASS registration system, as they must be identical. For more information about pivCLASS-compliant registration software, refer to pivCLASS documentation.
- Select the LP4502 panel name in the **Panel** field.
- Ensure the **Assurance Profile** field is updated as follows.

  For LP4502 with AAM only; does not appear for external PAM. Select a pivCLASS security level appropriate for the pivCLASS compliant door at the site; for example, CAK (PIV).

  Each profile refers to a protected area that is defined by NIST SP 800-116, titled "A Recommendation for the Use of PIV Credentials in PACS," and is secured by an identification method in accordance with the FIPS 201 standard, titled "Personal Identity Verification (PIV) of Federal Employees and Contractors."

  For more information about each authentication method, refer to pivCLASS Service documentation.
- To support the selected **Assurance Profile** for a pivCLASS configured door, it is recommended to set the Door Mode to **Card Only**. Note also, the Disabled, Unlocked and Locked No Access door actions supercede the Assurance Profile.

# Adding Reader Templates

When adding a reader template, do the following:

- Ensure the **Baud Rate** for the pivCLASS reader is updated as follows:

> **Note:** It recommended to specify a **Baud Rate** that is higher than the default **9600** (default) rate and to lower the baud rate, if reader issues occur. In addition, end users should hold the pivCLASS card on the pivCLASS reader for more than 5 seconds for smooth operation.

# Assigning Large Encoded Formats to Panels

If the **Enable Large Encoded Card Format** checkbox is enabled, the **128 bit Large Encoded** and **200 bit Large Encoded** card formats are automatically generated for the panel:

- On the Door: Edit page, select the **Operations** tab and ensure a large encoded card format is assigned to the panel in the **Members** box under **Card Formats**.

# Viewing Identities and Tokens

When adding an identity, do the following:

**Note:** ACM identity management is not used to create pivCLASS users. However, you can view identities and their tokens. You must use the pivCLASS registration system to add these identities in the ACM system. For more information about using pivCLASS-compliant registration software to add identities to the ACM system, refer to pivCLASS documentation. After these identities have been added, they can be searched, edited and modified to provide physical and logical access. If necessary, you can produce and print badges, assign to groups, roles, delegations, and so on, as you can for any other identity.

When viewing a token for an identity the following fields are read-only:

- The **Token Type** field displays **PIV** for a Personal Identification Verification (PIV) card for government employees or PIV-I for a PIV-Interoperable (PIV-I) card for government contractors.
- For PIV-I card only. The **CHUID** field displays the Card Holder Unique Identifier of the PIV-I card.

# Monitoring Events

You can monitor pivCLASS events on the Monitor Events page.

**Note:** pivCLASS events may be configured from **Physical Access** > **Events** and searching on **Name:** contains pivCLASS.

# Glossary

## 2

### 2-person control

Under this rule, all access and actions requires the presence of two authorized people at all times. Two people are necessary to either enter or exit a door.

## A

### ACM

Access Control Manager. Available in Enterprise, Enterprise Plus, Professional and Virtual Appliance platforms.

## B

### Badge template

The format designed for a user badge on which information from the Identities feature is placed. Templates are designed using the Badge Designer.

### BLE

Bluetooth Low Energy, a wireless communication protocol.

## C

### CHUID

Card Holder Unique Identifier. Used in PIV-I cards.

### CoS

Change of State

## D

### Debounce

Due to mechanical properties of a switch, when a switch is closed, there is a period of time in which the electrical connection "bounces" between open and closed. To a microcontroller, this "bouncing" can be interpreted as multiple button pushes. To suppress the "bouncing", the controller software is designed to anticipate it. This is known as "debouncing a switch".

### dogging

The action of turning the hex key and pressing the push bar to retract the latchbolt, which unlocks the perimeter door on the outside and allows a person to enter the building. Can be done remotely or manually.

### Door contacts

Input devices that detect changes in door position. This is generally done by measuring resistance across a circuit connecting part of the door jamb to the door itself. If the door is opened, the resistance drops.

### DPOS

Door position switch. These input devices are more commonly called door contacts.

## E

### EOL

End-Of-Line (EOL) are resistors that supervise the wiring between the alarm panel and the switch. Preset resistance levels must be maintained at input points or an alarm event is triggered.

## F

### Failover

When an appliance fails, a configured standby appliance is able to automatically, or manually, take its place so that the system can continue to run.

### FAS-N

Federal Agency Smart Credential Number. A 32-character number generated for FASC-N or CHUID for PIV-I cards.

### FIPS

Federal Information Processing Standard. The U.S. government's security standards for approving cryptographic modules and personnel identification methods. Only Mercury LP-series controllers with NIST certificate #2389 support the cryptographic module. Compliance requirements include: FIPS Publication 140-2 — a U.S. government computer security standard for approving cryptographic modules, titled "Security Requirements for Cryptographic Modules"; FIPS Publication 201-2 — a U.S. government standard for identifying federal government personnel, titled "Personal Identity Verification (PIV) of Federal Employees and Contractors."

### Flow control

The process of managing the rate of data transmission between two  nodes to prevent a fast sender from over running a slow receiver.

## I

### Interlock

A defined action that occurs within a panel at a destination device whenever an event occurs at the source device. For example, a REX input device (source); receives a request to exit and passes the order to the door strike device (destination); to open the door latch. For each interlock, a source and a destination device (or group of devices) is defined.

## L

### LDAP

Lightweight Directory Access Protocol is an open, industry standard application protocol for accessing and maintaining distributed directory information services over a network. An LDAP database in the Access Control Manager system typically includes user details, connected hardware details, events, alarms and other system configuration details.

## M

### Mag Lock

Magnetic locks work only with DC current, usually 12 to 24 volts. Never connect a magnetic lock to AC current of any voltage. All magnetic locks are fail safe. This means that they need a constant source of current to remained locked. If power is removed the lock will open. If this is a concern use a back-up power supply. All magnetic locks are silent even when powered and locked. 300 pound pull magnetic locks work well in light duty installations such as cabinetry.

## N

### Netmask

In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address(IP) so that only the host computer part of the address remains. The binary 1's at the beginning of the mask turn the network ID part of the IP address into 0's. The binary 0's that follow allow the host ID to remain. A frequently-used netmask is 255.255.255.0. (255 is the decimal equivalent of a binary string of eight ones.) Used for a Class C subnet (one with up to 255 host computers), the \".0\" in the \"255.255.255.0\" netmask allows the specific host computer address to be visible.

### NIST

National Institute of Standards and Technology. The U.S. government's standards body for approving software cryptographic modules in door controllers and personnel identification methods. Standards include: NIST SP 800-116, "Using Personal Identity Verification (PIV) Credentials In Physical Access Control Systems (PACS)"; NIST SP 800-131A, "Transitioning the Use of Cryptographic Algorithms and Key Lengths."

## P

### PACS

Physical Access Control System. An access control solution for securing people, property and assets. ACM is a PACS.

### Panel

Panels are controllers that connect to one or more doors (door controllers) and their associated readers, inputs, and outputs.

### PIV

Personal Identification Verification. A card issued to U.S. government employees and includes FASC-N information.

### PIV-I

PIV - Interoperable. A card issued to U.S. government contractors and includes CHUID and FASC-N information.

### Postgres

An object-relational database management system (ORDBMS) available for many platforms including Linux, FreeBSD, Solaris, Microsoft Windows and Mac OS X. Also callsed PostgreSQL.

## R

### redundancy

see Failover

### Replication

The process of copying and synchronizing the LDAP database between two or more appliances so that they share the same configuration information.

### REX

Request to exit. REX devices include crash bars and exit buttons.

### RQE

Request to exit. Normally these are crash bars or buttons.

### RTN

Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

## S

### SCP

Secure Copy Protocol is the most basic backup protocol and does not require much adjustment before it can work properly. It can work effectively on Linux and other Unix-like systems. To start work, its enough to install the SCP program on the server and establish the connection.

### SFTP

Secure File Transfer Protocol is a network protocol that provides file management functionality over any reliable data stream. This protocol assumes that it is run over a secure channel, such as Secure Shell Protocol (SSH), that the server has already authenticated the client, and that the identity of the client user is available to the protocol.

### SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

### SNMP

A UDP-based network protocol used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

### Strike

Electric strikes are often used for "buzz in" types of systems. Electric strikes come in many varieties. They can be 12 or 24 volts or even higher voltage and they may take AC or DC current and some even take both. They may be fail safe or fail secure. A fail safe electric strike needs power to keep it locked. A fail secure

electric strike stays locked even without power. The most common by far is a fail secure.

### Subpanels

If your system supports a hierarchical structure, subpanels are specialty panels that are controlled by a primary panel. One primary panel can be connected to a large number of specialty subpanels, incorporating an array of devices such as single and multiple door modules, keypads, input modules and output modules.

## T

### TLS

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which are designed to provide communication security over the Internet.

### Token

The entry data required to enable an employee or visitor to access a location. This typically includes a PIN number and, if a physical badge or keycard is required, a number on the card.

## U

### undogging

The action of turning the hex key and releasing the push bar to extend the latchbolt, which locks the perimeter door on the outside and prevents a person from entering the building. Can be done remotely or manually.