

Admin Guide

Access Control ManagerTM Software

Version 5.12.2

© 2016- 2019, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo, AVIGILON 5.12.2, ACC, ACCESS CONTROL MANAGER, ACM and ACM VERIFY are trademarks of Avigilon Corporation. HID, HID GLOBAL, APERIO and VERTX are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US 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. Other names or logos mentioned herein may be the trademarks of their respective owners. The absence of the symbols TM and ® in proximity to each trademark in this document or at all is not a disclaimer of ownership of the related trademark. Avigilon Corporation protects its innovations with patents issued in the United States of America and other jurisdictions worldwide (see [avigilon.com/patents](https://www.avigilon.com/patents)). Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Avigilon Corporation or its licensors.

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-5.12.2-A

Revision: 1 - EN

20190220

Table of Contents

Introduction	14
Monitoring	15
Monitoring Events	15
Pause/Resume Events	16
Clear Events	16
View Live Video	16
View Recorded Video	17
Create Event Notes	17
View Event Notes	18
View Event Instructions	18
View Event Identity Details	18
View Event History	19
Change Events List Settings	19
Reconnect to Events List	19
Searching for Events and Alarms	20
View Camera (Search)	21
View Recorded Video (Search)	21
Create Event Notes (Search)	22
View Event Notes (Search)	22
View Event Instructions (Search)	23
View Event Identity Details (Search)	23
View Event History (Search)	23
Change Transactions List Settings	24
Monitor Alarms	24
Acknowledge Alarms	25
View Live Video (Alarms)	25
View Recorded Video (Alarms)	26
Create Event Notes (Alarms)	26
View Event Notes (Alarms)	27
View Event Instructions (Alarms)	27
View Event Identity Details (Alarms)	27
View Event History (Alarms)	28
Change Alarms List Settings	28
Monitor - Verification screen	29
Verifying Identities at Doors	29

Verification Events List	30
Monitor - Dashboard	31
Panels table	32
Doors table	33
LifeSafety Panels table	35
Controlling System Hardware	36
Status Colors	37
Monitor Screen - Map Templates page	38
Using a Map	38
Add Map	41
Monitor Intrusion Panels	41
Monitor Intrusion Panel Status	41
Monitor Intrusion Panel Areas	42
Monitor Intrusion Panel Points	43
Monitor Intrusion Panel Outputs	44
Identities	46
Searching for an Identity	46
Adding an Identity	47
Identities - Assigning Roles	48
Identities - Assigning Tokens	49
Identities - Assigning Groups	49
Capturing and Uploading Photos of an Identity	50
Identities - Creating Badges	55
Timed Access	55
Adding Timed Access to an Identity	57
Editing Timed Access	57
Deleting Timed Access	57
Editing an Identity	58
Reports	59
Reports - Generating Reports	59
Reports - Report Preview	59
Reports - Editing	60
Reports - Editing Audit Log and Transaction Reports	61
Reports - Creating Custom Reports	62
Reports - Creating Custom Audit Log and Transaction Reports	63
Physical Access	64

Configuring Templates (Mercury Security)	64
Door Templates	65
Door Templates - Batch Update	65
Door Templates list page	66
Door Templates - Add page	66
Door Templates - Edit page	68
Door Templates - Batch Update	70
Reader Templates	71
Reader Templates list page	71
Reader Template: Add page	71
Reader Template: Edit page	74
Input Templates	77
Input Templates list page	77
Input Template: Add page	77
Input Template: Edit page	79
Output Templates	80
Output Templates list page	81
Output Template: Add page	81
Output Template: Edit page	82
Wiring Templates	83
Wiring Templates list page	83
Wiring Template: Add page	83
Wiring Template: Edit page	84
Configuring Panels	85
Searching for Panels	86
Adding Panels	86
Configuring the Mercury Security MS Bridge Solution	87
Batch Creating Subpanels on a New Mercury Panel	87
Subpanel: Batch Create page (Mercury Security)	88
Subpanel: Batch Edit Details page (Mercury Security)	89
Subpanel: Batch Name Doors or Subpanel: Batch Create Summary page (Mercury Security)	90
Adding HID VertX® Subpanels	90
Adding Mercury Security Panels	90
Editing Panels	91
Editing HID® VertX® Panels	91
Editing Mercury Security Panels	91

Resetting Anti-Passback from the Panel	92
Downloading Parameters	92
Downloading Tokens	92
Lenel Panel Support	92
Resetting Doors/Subpanels	93
Updating Panel Firmware	93
Updating Panel Time	94
Deleting Panels	94
Configuring Subpanels	94
Adding a Subpanel	95
Editing Subpanels	96
Inputs	96
Output Operating Modes	97
Outputs	97
Deleting Subpanels	98
Macros	98
Adding Macros	99
Editing Macros	99
Deleting Macros	99
Assigning Macros	99
Assigning a Macro to a Trigger	100
Assigning a Macro to a Macro	100
Assigning a Macro to a Door	100
Sorting Macros	100
Triggers	101
Adding Triggers	101
Editing Triggers	101
Deleting Triggers	101
Configuring Doors	101
Searching for Doors	102
Advanced Filtering on the Doors List	103
Controlling Doors	103
Adding Doors	104
Adding Simple Macros	106
Editing Doors	106
Doors - Editing VertX® Doors	107
Doors - Editing Mercury Security Doors	107

Deleting Doors	108
Door Modes	108
Access Types	108
Anti-Passback	109
Anti-Passback Modes	109
Setting Up Anti-Passback	110
Granting a Free Pass	111
Global Anti-Passback	112
Global Anti-Passback Modes	112
Interlocks	113
Adding Interlocks	115
Editing Interlocks	115
Configuring Locks	115
Configuring Assa Abloy Aperio® Wireless Lock Technology	115
Configuring Allegion Schlage AD400 Series Locks	116
Configuring Allegion Schlage LE Series Locks	117
Configuring Allegion Schlage NDE Series Locks	118
Configuring SimonsVoss Wireless Locks	119
Doors list	123
Door: Add page	125
Options for an Avigilon Door	127
Options For VertX® and Mercury Security Doors	127
Door Processing Attributes for VertX® Doors	128
Door Processing Attributes for Mercury Security Doors	129
Doors - VertX® New Parameters page	130
Doors - Mercury Security New Parameters page	132
Doors - Edit Screen	135
Door: Edit page (VertX®)	135
Parameters tab (VertX®)	135
Operations tab (VertX®)	137
Hardware tab (VertX®)	140
Reader Edit page (VertX®)	142
Input Edit page (VertX®)	143
Output Edit page (VertX®)	144
Cameras tab (VertX®)	144
Events tab (VertX® doors)	146
Doors - Creating Local Events for VertX® Doors	147

Access tab (VertX®)	148
Transactions tab (VertX®)	149
Door: Edit page (Mercury Security)	149
Parameters tab (Mercury Security)	149
Operations tab (Mercury Security)	152
Hardware tab (Mercury Security)	156
Reader Edit page (Mercury Security)	158
Input Edit page (Mercury Security)	161
Output Edit page (Mercury Security)	162
Elev tab (Mercury Security)	162
Cameras tab (Mercury Security)	163
Live Video Window	165
Interlocks tab (Mercury Security)	165
Interlocks Add page	167
Interlock Edit page	169
Events tab (Mercury Security doors)	170
Doors - Creating Local Events for Mercury Security Doors	171
Access tab (Mercury Security)	172
Transactions tab (Mercury Security)	173
Doors - Access page	173
Configuring ACM Verify™ Virtual Doors	173
Adding an ACM Verify Door	173
Parameters tab (Avigilon)	174
Paired Devices	175
Prerequisites for Pairing Devices	176
Precautions for Paired ACM Verify Stations	176
Pairing a Device	176
Using ACM Verify	177
Configuring Areas	178
Adding Areas	180
Areas - Editing	180
Areas - Deleting	180
EOL Resistance	180
Adding EOL Resistance for Mercury Input Points	181
Adding EOL Resistance for VertX® Input Points	181
Editing EOL Resistance for Mercury Input Points	181
Editing EOL Resistance for VertX® Input Points	181

Mercury LED Modes - List page	181
Editing Mercury Security LED Modes	182
Mercury Security LED Mode Table page	182
LED Modes for Mercury Security	183
Configuring Card Formats	185
Adding Card Formats	186
Editing Card Formats	186
Deleting Card Formats	186
Configuring ACM System Events	186
Searching for ACM System Events	187
Customizing ACM System Events	187
Assigning Priority Colors to ACM System Events	187
Global Actions	189
Global Actions - Adding	189
Global Actions - Editing	189
Global Actions - Action Types	189
Global Actions - Deleting	190
Global Actions - Intrusion Linkages and Actions	190
Intrusion panel alarm due to an event in the ACM System	190
Disable/enable doors from keypad	190
Disarm Alarm on Access Grant with restricted authorities	191
Global Linkages - Introduction	191
Global Linkages - Adding	192
Global Linkages - Editing	192
Mustering - Introduction	192
Mustering - Requirements	192
Mustering - Creating a Dashboard	193
Mustering - Using the Dashboard	194
Mustering - Manually Moving Identities	196
Managing Appliances	197
Appliances - Changes	197
Adding Extra Appliances	197
Editing Appliances	197
Deleting an Appliance	198
Configuring Replication and Failover	198
Failover/Redundancy Feature	199
Automatic failover	199

Manual failover and failback	200
Recommended System Architecture	200
System Architecture for Replication	200
System Architecture for Redundancy	201
Replication and Failover Requirements	203
1. Preparing Appliances for Replication and Failover	205
Setting Up the Primary Appliance	205
Setting Up Additional Appliances	206
2. Setting Up Replication Between Appliances	208
Enabling Replication on the Primary Appliance	208
Enabling Replication on the Second Peer or Standby Appliance	209
3. Adding a Replication Subscription	210
Testing Replication	213
Checking the Appliance Replication Status	214
Testing Two-Way Replication	215
4. Setting Up Failover	216
Configuring Email Notifications for Replication Events	218
Removing Replication and Failover	219
Failing Over and Failing Back	219
Automatic Failover	220
Manual Failover	220
Failback	221
Monitoring Transactional Replication to Hot Standby	222
Configuring Network Connections	222
Configuring Ethernet Ports	222
Adding Ethernet Routes	223
Enabling Serial Ports	223
Backups	224
Backing Up System Data	224
Manually Backing Up Data	225
Restoring Backups	225
Restoring Backups From Other Backup Events	226
Logs	227
Accessing Appliance Logs	227
Software Updates	227
Updating the Appliance Software	227
Viewing the ACM SSL Certificate	228

Appliances - About	229
Applying License Upgrades	229
Viewing the End User License Agreement	229
Accepting the End User License Agreement	229
Reviewing the Appliance Status	230
Managing Collaborations	231
Collaborations - Adding	231
Collaborations - Adding Events XML Collaboration	232
Collaborations - Events XML Definitions	233
Collaborations - Events XML Example	236
Collaboration - Editing	238
Collaboration - Types	238
Collaboration - Running	239
Collaboration - Deleting	239
Collaboration - Assigning Events to a Collaboration	239
Setup & Settings	241
Schedules and Holidays - Introduction	241
Schedules	241
Holidays	242
Adding Schedules	242
Editing Schedules	243
Deleting Schedules	243
Holidays - Adding	243
Holidays - Editing	244
Holidays - Deleting	244
Holidays and Schedules - Examples	244
Example 1: Part-Day Holiday	244
Example 2: Additional Access Time	245
Event Types - Introduction	246
Adding Event Types	248
Editing Event Types	248
Deleting Event Types	248
User Defined Fields - Introduction	248
User Defined Fields - Adding a Field	249
User Defined Fields - Adding User Defined Tabs	249
User Defined Fields - Editing User Defined Tabs	250

User Defined Fields - Deleting Fields	250
User Defined Tabs - Deleting	251
User Lists - Introduction	251
User Lists - Adding Items to a List	251
User Lists - Editing Items	251
User Lists - Deleting Items	252
System Settings	252
System Settings - General page	252
Remote Authentication from External Domains	255
About Certificate Pinning	256
System Settings - Configuring Remote Authentication Using SSL Certificates	256
Using Pinned Certificates	256
Using Trusted Certificates	257
System Settings - Remote Authentication	259
Badge Templates and the Badge Designer	259
Using the Badge Designer	260
Badge Templates - listing page	265
External Systems - Introduction	266
External Systems - Adding	266
External Systems - Editing	266
External Systems - Deleting	266
External Systems - Integrating an ACM Appliance into an ACC™ Site	267
External Systems - Defining the Badge Camera for the System	269
Bosch Intrusion Panels	269
Adding a Bosch Intrusion Panel	269
Editing a Bosch Intrusion Panel	270
Synchronizing Bosch Intrusion Panels	271
Deleting a Bosch Intrusion Panel	271
Viewing Bosch Intrusion Panel Areas	271
Viewing Bosch Intrusion Panel Points	271
Viewing Bosch Intrusion Panel Outputs	272
Viewing Bosch Intrusion Panel Users	272
Assigning Bosch Intrusion Panel Users to Identities	272
Supported Bosch Intrusion Panels	273
External Systems - ViRDI	276
External Systems - ViRDI System Settings	276
Maps - Introduction	277

Maps - Creating and Editing a Map	277
Maps - Linking Maps	278
Using a Map	279
Priority Situations	282
Planning Priority Door Policies	282
Priority Door Policies, Global Actions, and Modes	283
Priority Door Policies and Emergencies	284
Configuring a Secure High-Priority Emergency Response	285
Testing a Secure Priority Emergency Response in the ACM System	287
Activating the High-Priority Emergency Response	288
During a High-Priority Situation	289
Deactivating a Priority Door Policy	290
Limitations of Priority Global Actions	290
Priority Hierarchy	291
Overriding Door Modes and Schedules	293
Adding an Override	293
Accessing the List of Overrides	294
Monitoring Overrides	295
Modifying and Deleting Overrides	295
Modifying an Override	296
Setting Personal Preferences	297
Changing the Password in My Account	297
Scheduling Batch Jobs	297
Generating a Batch Report	297
Applying an Identity Profile to a Group Using a Job Specification	299
Applying a Door Template to a Group Using a Job Specification	301
Scheduling a Global Action	303
Setting Batch Door Modes	304
Permissions and Rights	306

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 oversees the ACM system. They are responsible for monitoring and maintaining the ACM system. For more information, see *Permissions and Rights* on page 306.

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

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 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 cardholder to the system, etc. In other words, any transfer of data within the system is an event.

When you click **Monitor**, the first page you see is the Events page. This page lists all the events or transactions as they occur in the system.

To review the events as they appear on the Events page, use any of the following buttons:

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

- **Pause** — Click this button 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**.
- **Resume** — Click this button to restart the flow of events that are displayed on the page.
This button only appears when the flow of events is paused.
- **Clear** — Click this button to 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** — Click this button to display live video that is associated with the selected event.
- **Recorded Video** — Click this button to display recorded video that is associated with the selected event.
- **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 event occurs. The instructions were added when the event was created.
- **Identity** — Click this button to display details about the person that triggered the selected event.
- **History** — Click this button to display a detailed history of this event.
- **Save Settings** — Click this button to save your current settings for this page. For example, the columns and order for this page.

- **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.

Click and drag the columns to move them into the order you want.

- **Reconnect** — Click this button to reconnect 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 page 15).
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 15).
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 15).
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 15).
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 15).
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 15).
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 Listing page.

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 Access Control Manager appliance.

1. Click **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 15).

If your browser loses connectivity with Access Control Manager 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**.

The Events Search (Transactions) page appears.

2. Scroll to the bottom of the page and click the  icon.

The Search area is displayed:

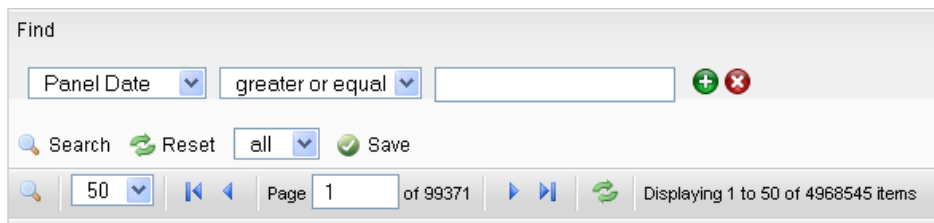


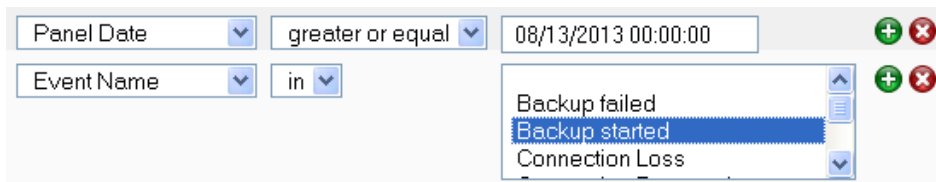



Figure 1: Search options

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.




7. Add as many search filters as you need to fulfill your search criteria.
8. When you have entered all your search criteria, click  **Search**. The search results are listed in the table above the search area.
9. 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**. The Events Search (Transactions) page displays.
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 24.

3. Click **Camera** to display live video that is associated with the selected event.

The Monitor Screen - Live Video window displays.

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**. The Events Search (Transactions) page displays.
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 24.

3. Click **Recorded Video** to display recorded video that is associated with the selected event.

The Monitor Screen - Recorded Video window displays.

NOTE: Events 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**. The Events Search (Transactions) page displays.
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**. The Events Search (Transactions) page displays.
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**. The Events Search (Transactions) page displays.
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**. The Events Search (Transactions) page displays.
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**. The Events Search (Transactions) page displays.
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

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

1. Click **Monitor > Search**. The Events Search (Transactions) page displays.
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. Click **Save Settings** if you want to save the new settings.

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

Monitor 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.
- **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 noises 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**. The Monitor Alarms Listing page displays.
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.

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**. The Monitor Alarms page displays. For more information see *Monitor Alarms* on page 24.
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 Listing page.

1. Click **Monitor > Alarms**. The Monitor Alarms page displays (for more information see *Monitor Alarms* on page 24).
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 *Monitor Alarms* on page 24.
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 *Monitor Alarms* on page 24.

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 *Monitor Alarms* on page 24.

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 *Monitor Alarms* on page 24.
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 *Monitor Alarms* on page 24.
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 *Monitor Alarms* on page 24.

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.

Monitor - Verification screen

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.

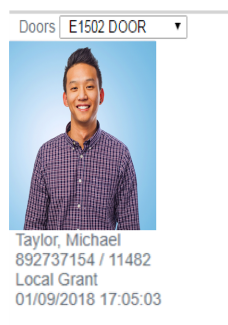
Not all door events will display in this list. Only events in the priority number range 300 to 700 display. A full listing of all events is available on the Monitor Events page.

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 there is one . 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.


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.

Monitor - Dashboard

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

Select **Monitor > Dashboard** to open it. Use the navigation sidebar to move between the  Dashboard, the  Panels table, the  Doors table, and the  Power Supplies table (if a LifeSafety power supply is connected).

With the Dashboard open, you can immediately respond to hardware faults or unexpected input/output state changes as they occur. As the status of hardware components change, the status indicators on the Dashboard change color.





For each category, the total number of connected components (installed and uninstalled) is displayed above a real-time fault or status list. For the panel, subpanel, or door categories, the number of installed components in each fault state is displayed. When there are no faults for a panel, subpanel, or door item, the status is green. There are no fault states for inputs or outputs; the numbers indicate the number of installed inputs or outputs in each state. When there are no components in a state, the status is either green or 0.

When numbers appear next to an item you can drill down into the Dashboard tables for more information:

- **Panels**—Summarizes the fault state of the installed panels. Click on the number next to the fault to open the Panels table filtered to display only the panels with that fault for more details.
- **Subpanels**—Summarizes the fault state of the installed subpanels. To see the subpanels in a fault state, click on the corresponding fault under Panels, then click on the panel name in the Panels table to expand the Subpanels table to list the subpanels with that fault for more details.
- **Inputs and Outputs**—The number indicates how many inputs or outputs are in each state. There are no fault states for inputs or outputs. To see details about input or output states, expand each subpanel on the Panels tab.
- **Doors table**—Summarizes the fault state of the installed doors. Click on the number to drill down to the **Doors** table filtered to display only alarms for more details.
- **Appliances**—When there are no issues with the ACM appliance items, their status is green. Hover the mouse over each status indicator to see more details.

When a Panels or Doors table is accessed from the navigation sidebar, or by clicking on the Panels or Doors total value, the table lists all connected panels or doors. When accessed by clicking on a fault count value number, the table lists only the panels or doors experiencing active faults of that type.

The color applied to icons in the Dashboard tables indicate the status of the hardware component.

Color	Status	Description
	Normal	Online and working properly.
	Trouble	Indeterminate status. Seen for inputs, outputs, and the ACM appliance.
	Alarm	Alarm condition. An ACM operator should investigate the problem and resolve the issue.
	Masked	Input is currently masked. Its actual state is not displayed. Mask inputs that are intended to change as part of normal operations, so that they are not constantly being reported.

Panels table

Access the Panels table to install, uninstall, and delete panels and to see more information about the state of individual panels. From the Panels table, you can access a panel's Subpanels table. From the Subpanels table you can access a subpanel's Inputs and Outputs tables.

When it is accessed from the navigation sidebar of the Dashboard panel, or by clicking the total value for panels in the dashboard, the Panels table lists all of the panels connected to the ACM appliance (whether installed or installed). When it is accessed by clicking on a number next to a panel fault, the Panels table lists the panels experiencing active faults of that type.

Installing, uninstalling, or deleting a panel or subpanel:

Click  at the end of a row in the Panels table or Subpanels table to complete any of the following actions:


- Install—enables communications between the panel or subpanel and the ACM system.
- Uninstall—disables communications between the panel or subpanel and the ACM system.
- Delete—removes the connection between the panel or subpanel and the ACM system.

Masking and unmasking inputs:

Click  at the end of a row in the Inputs table to complete any of the following actions:

- Mask — Masks the specified input.
- Unmask — Click this button to unmask a previously masked input.

Masking and unmasking inputs:

Click  at the end of a row in the Outputs table to complete any of the following actions:

- On — Power the output. If this output is a door, it energizes the circuit.
- Off — Turn off the power to this output. If this output is a door, it de-energizes the circuit.
- Pulse — Alternately energize and de-energize this output. The pulse interval is determined by the output's settings.

Checking the status of a panel, its subpanels, and its inputs/outputs:



- Click on the name of the panel to expand the Subpanels table.

- Click on the name of a subpanel to expand the Inputs and Outputs tables.

Searching the Panels table:

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 Panels list is filtered to show the results of your search.

Sorting the Panels table:

1. Click in a column heading:
 - Click  to sort in ascending order.
 - Click  to sort in descending order.

To see the legend for panel statuses:

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



Doors table

Access the Doors table to control individual doors, investigate doors with active faults, and see more information about the state of individual doors.

When it is accessed from the navigation sidebar of the Dashboard panel, or by clicking the total value for doors in the dashboard, the Doors table lists all of the doors connected to the ACM appliance (whether installed or installed). When it is accessed by clicking on a number next to a door fault, the Doors table lists the doors experiencing active faults of that type.

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**
 - **Grant** — Momentarily unlocks this door for the standard access time.
 - **Restore** — Resets the door mode to its configured value. If the door is in any privacy mode (Privacy, or Apartment) it will be 'restored' to the non-privacy mode (e.g. if the door is in Privacy mode, and the Restore option is selected then the mode return to its configured value).
 - **Unlock** — Unlocks the door. This door will remain unlocked until the **Restore** command is issued, or until another change of state is directed, either via operator override or scheduled action.
 - **Locked No Access** — Locks the specified door and denies access for all card reads. This door will remain locked until the **Restore** command is issued, or until another change of state is

directed, either via operator override or scheduled action.

- **Disable** — Disables the specified door. This keeps it from operating and allows no access.

- **Door Mode**

- **Card Only** — This door can be accessed using a card. No PIN 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.
- **Pin Only** — This door can only be accessed by entering a PIN at a keypad. No card is required.
- **Facility Code Only** — This door can be accessed using a facility code.

The Pin only and Card or Pin door modes are not available if the 'Allow duplicate PINs' option was selected on the System Settings - General page when this appliance was configured.

- **Forced**

- **Mask Held**—Masks the Door Held Open alarm for this door. The status color changes to blue and is no longer included in any alarm subtotal.
- **Unmask Held**—Unmasks the Door Held Open alarm for this door.

- **Held**

- **Mask Forced** — Masks the Forced Door Alarm for this door.
- **Unmask Forced** —Unmasks the Forced Door Alarm for this door.

- **Installed**

- **Install** — Installs a door. Enables communications between the door and the ACM system.
- **Uninstall** — Uninstalls a door. Disables communications between the door and the ACM system.

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 Doors table:

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 that includes multiple filters:

1. Click **Advanced Filters**.

2. Select filters:

- **Alarms**—Select the alarms to include from the list of alarms.
- **Masked**—Select 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 Doors table:

1. Click in a column heading:

- Click  to sort in ascending order.
- Click  to sort in descending order.

To see the legend for all door statuses:



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

There are three groupings which are color-coded — Normal , Alarms , Masked  :

LifeSafety Panels table

When LifeSafety 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  **Power Supplies** in the Dashboard navigation sidebar to open the LifeSafety Panels table.

Option	Description
Name	The name of the LifeSafety panel. Click this name to display the panel details.
Installed	The status of the panel's installation:  (installed) or  (uninstalled). This field is not selectable and cannot be toggled.
Commands	The commands available to control a LifeSafety panel: <ul style="list-style-type: none">• Status — Click this button to display the current status of the displayed LifeSafety panel.• Log — Click this button to view the log of events/alarms recorded by the LifeSafety panel.• Edit — Click this button to open the browser page for this remotely connected panel and make changes to the configuration as required. The page displayed is determined by the URL specified on the Address field of the LifeSafety Add page.

Controlling System Hardware

While you are monitoring the system, you may sometimes need to override the default door settings to allow a visitor access to an area, or unlock a door in an emergency situation. You can control doors from the Dashboard:

1. Select **Monitor > Dashboard**.
2. Click **Doors** in the Dashboard navigation area.
3. Check the box beside each door you want to control, and use any of the following to change the settings:
 - Click the **Door Action** dropdown, then:
 - Click **Disable** to stop the door from operating and allow no access.
 - Click **Unlock** to unlock the door. This door will remain unlocked until the Restore command is issued, or until another change of state is directed, either via operator override or scheduled action.
 - Click **Locked No Access** to lock the door. This door will remain locked until the Restore command is issued, or until another change of state is directed, either via operator override or scheduled action.
 - Click **Grant** to momentarily grant access to the door to permit a single-time entry.
 - Click **Restore** — Click this button to reset the door mode to its configured value.
 - Click the **Door Mode**, then choose how access is controlled at the door:
 - Card Only
 - Card and Pin
 - Card or Pin
 - Pin Only
 - Facility Code Only

The Pin only and Card or Pin door modes are not available if the 'Allow duplicate PINs' option was selected on the System Settings - General page when this appliance was configured.

- Click the **Held** dropdown, then:
 - Click **Mask Held** to mask the Door Held Open alarm for this door. The status color changes to blue and is no longer included in any alarm subtotal.
 - Click **Unmask Held** to unmask the Door Held Open alarm for this door.
- Click the **Forced** dropdown, then:
 - Click **Mask Forced** to mask the Door Forced Open alarm for this door. The status color changes to blue and is no longer included in any alarm subtotal.
 - Click **Mask Unforced** to unmask the Door Forced Open alarm for this door.

4. To change the door mode, Click **Door Mode**, then choose from the following options:

- Card Only
- Card and Pin
- Card or Pin
- Pin Only
- Facility Code Only

NOTE: The Pin only and Card or Pin door modes will not be available if the 'Allow duplicate PINs' option has been selected on the System Settings - General page.



5. To control an input:

- In the Panel Status area, click the name of the connected panel then click the name of the connected subpanel.
- When the required input is displayed, click one of the following buttons:
 - **Mask** — Click this button to mask the specified input.
 - **Unmask** — Click this button to unmask a previously masked input.

6. To control an output:

- In the Panel Status area, click the name of the connected panel then click the name of the connected subpanel.
- When the required output is displayed, click one of the following buttons:
 - **On** — Click this button to power the output.
 - **Off** — Click this button to turn off the power to this output.
 - **Pulse** — Click this button to alternately energize and de-energize this output. The pulse interval is determined by the output's settings.




7. To install or uninstall a door or subpanel, click on the existing icon (e.g. if Installed is the current status,


click on the installed icon  to change the status to  Uninstalled).

The action is performed on the specified device.

Status Colors

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

Color	Description
 Normal	The Access Control Manager component is online and working properly.
 Trouble	The Access Control Manager component has an indeterminate status.
 Alarm	The Access Control Manager component is experiencing an alarm condition. The delegated operator should investigate the problem and resolve the issue.

Color	Description
 Masked	The specified Access Control Manager input is currently masked. Its actual state is not displayed. Mask inputs that are intended to change as part of normal operations, so that they are not constantly being reported.

Monitor Screen - Map Templates page

When you click **Monitor > Maps**, the Map Templates page displays. This page lists all the maps that have been added to the system.

Feature	Description
Add New Map Template	Click this button to add a new map template.
Name	<p>The name of the map template.</p> <p>A list of all the configured maps is displayed. Also included in the list are configured Mustering dashboards.</p> <p>Click the name of the map template to display the configured map or dashboard.</p>





Using a Map

After a map has been configured, access it from the Monitor page and use it as a quick visual reference to all the items that may be installed in a facility.

From the map, you can:

- Monitor the status of hardware items: doors, panels, subpanels, inputs and outputs.
- Control doors.
- Keep track of identities as they arrive at muster stations from the Mustering dashboard.

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

- : A green bar indicates the hardware item is operating normally.
- : A red square indicates the hardware item is in an alarm state. The counter in the square shows the number of unacknowledged events.
- : A solid blue disk indicates an active override is in effect on the door. A hollow blue disk indicates an inactive override is defined. For more information, see
- : A red bounding box is displayed around the status bar of a door in Priority Mode.









To access and monitor your site from a map:


1. Select **Monitor > Maps**. The Map Templates page displays.
2. In the Map Templates Listing page, click the name of a map.

The map is displayed. Some of the displayed elements may not appear in your map or the example below.






Figure 2: Example map

Feature	Map Icon
Doors	
Panels	
Subpanels	
Inputs	
Outputs	
Cameras	
Zoom In	
Zoom Out	

Feature	Map Icon
Global Actions	
Dashboard Elements	Square, circle or text object

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


To...	Do this...
Review hardware status	<p>The colored bar below each item displays an overview of the current communication and power status. Click the icon on the map to display the control menu.</p> <p>For more information about the colored hardware status bar, see the specific hardware status page.</p> <p>For more information about the status colors, see <i>Status Colors</i> on page 37.</p>
Review an alarm	<p>If you see a red alarm indicator, the item on the map is in an alarm state. Click the alarm indicator to see the status details.</p> <p>For more information about alarm actions, see <i>Monitor Alarms</i> on page 24.</p>
Modify or delete an override	<p>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. Click the indicator to open the <i>Doors: Overrides</i> page to see details.</p>
Respond to a priority situation	<p>If you see a red bounding box around the status indicator, the door is in Priority Mode.</p> <p>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.</p>
Display video	<p>Click the  on the map to display the Camera Video window.</p>
Open a linked map	<p>Click  to display a linked map, or  to display a linked map.</p>
Monitor the dashboard	<p>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.</p> <p>The dashboard displays the number of identities in the area and may include the name of the area. In <i>Example map</i> on the previous page, the dashboard is the gray square.</p> <p>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.</p>

Add Map

Follow the steps below to add maps.

1. Click **Monitor > Maps**. The Map Templates (Monitor) Listing page displays.
2. Click **Add New Map Template**.

The **Map Template: Add New** page displays.

3. Enter a name for the Map in the Name field.
4. To:
 - upload a file, select **File** and click **Browse** then select the file to upload in the **Choose File to Upload** dialog box and click **Open**.
 - create a blank canvas, select **Blank Canvas**.
5. To resize the image, enter resizing proportions in the **Re-size To** fields.
6. Click  to save the map.

The **Map Template: Edit** page displays.

Monitor Intrusion Panels

The following procedures relate to monitoring Bosch intrusion panels.

Monitor 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 > Intrusion Status**.

The Monitor Intrusion Status - Panels screen displays.

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.

Monitor Intrusion Panel Areas

The intrusion panel areas display the current status for all defined areas. For example if an area is armed, the Armed status will display and a message will appear when you hover over the status icon.

To monitor intrusion panel area status and make updates as required:

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

The Monitor Intrusion Status - Areas screen displays.

3. View the list that displays. A status is displayed for each area.

The following statuses apply to all of the above:

 Armed

 Ready to Arm

 Not Ready to Arm

 Partial Arm

 Trouble

 Alarm

NOTE: To view more detail on the status, hover over the status icon to view a pop-up message (e.g. hovering over an Armed status indicator might return the message 'All On Instant Arm').

4. If you want to narrow the list that displays, either:
 - Use the filter function. Enter an area name to filter the list results by area. Type in the name (or part of the name) of the area or panel and the list will update as you type.
 - Select a single status (e.g. Partial Arm) 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. To arm an area:
 - Select the areas to be armed.
 - Click **Master** then select the arming option. Options are:
 - 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
7. To arm a perimeter area:
 - Select the areas to be armed.
 - Click **Perimeter** then select the arming option.
 - Instant Arm
 - Delay Arm
 - Force Instant Arm
 - Force Delay Arm
8. To disarm select the areas to be disarmed and click **Disarm**.
9. To silence intrusion alarms select the areas to be silenced and click **Silence**.
10. To reset the sensors select the areas to be reset and 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 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 > Intrusion Status**.
2. Click the **Points** tab.

The Monitor Intrusion Status - Points screen displays.
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 bypassable due to configuration settings. Trying to bypass these points will result in no state change.

Monitor Intrusion Panel Outputs

The 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 > Intrusion Status**.
2. Click the **Outputs** tab.

The Monitor Intrusion Status - Outputs screen displays.



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.

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.

Searching for an Identity

Use the Search feature to find an identity in the database.

1. The Search area is at the top of the Identity Search page. Fill out the following fields:
 - **Last Name** field.
 - (Optional) The **First Name** and/ or **Internal Number** fields.
 - (Optional) The Group field.
2. Add any additional search criteria as follows:
 - Select the criteria from the **Search Field** drop down list.
 - Enter or select the value to search for in the **Search Value** field.
 - Click **Add Criteria** to add an additional search, then repeat the steps in the bullets above for each additional criteria. Add as many search filters as you need to fulfill your search criteria.
 - At any time, you can click **Clear Search** to clear all fields.
 - To remove a single criteria row, click **Remove**.
3. In the drop down list to the right of the **Search** button, select whether the values entered in the fields should be combined into a single search criteria (**And**) or used as separate search criteria (**Or**).

If **And** is selected, only the identities that fit all entered criteria will appear. If **Or** is selected, the identities that fit one or more of the entered criteria will appear.
4. When you have entered all your search criteria, click **Search**.

The page refreshes and displays your search results.

NOTE: Always enter data in the Search Value field. Searching using blank entries will return all identities as the result.

Adding an Identity

When a new user needs access to the ACM 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.

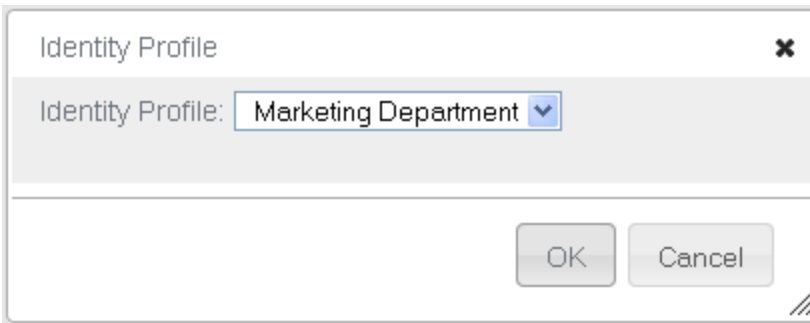
To add a new identity:

1. Click **Identities**.

The Identities Search page appears.

2. Click **Add New Identity**.

If you have defined one or more Identity Profiles for this system, the Identity Profile dialog box will pop up:

A screenshot of a dialog box titled "Identity Profile" with a close button (X) in the top right corner. Inside the dialog, there is a label "Identity Profile:" followed by a dropdown menu showing "Marketing Department" with a downward arrow. At the bottom right of the dialog are two buttons: "OK" and "Cancel".

- From the **Identity Profile** drop down list, select the profile you want to assign to this identity, then click **OK**.
- If you do not want to assign an identity profile to this identity, click **Cancel**.


The Identity Add page appears. The data from the Identity Profile will be populated on the screen.

3. Fill out the **Last Name** field, then complete the page with the required details.

NOTE: You can add additional values to some drop down lists using the User Lists feature.


4. Click .

When the page refreshes, you are automatically taken to the Roles page.

5. Assign roles to this identity as required, then click .

When the page refreshes, you are automatically taken to the Tokens page.

6. Enter the token details as required. By default the **Download** check box is selected. This downloads the token to the connected panels and associated doors.

When you are finished, click .

7. Navigate through the tabbed pages to add more details about the identity. The tabbed pages include:
 - **Roles:** use this page to assign a role to this identity.
 - **Tokens:** use this page to create a token for the identity.
 - **Groups:** use this page to assign this identity to a group.
 - **Capture:** use this page to take a photo of the user.
 - **Photos:** use this page to upload an existing photo of the user.
 - **Badge:** use this page to assign a badge to this user.
 - **Timed Access:** use this page to assign timed access to this user.
 - **Access:** use this page to view this identity's access privileges including roles, access groups, and doors.
 - **Transactions:** use this page to view transactional data associated with the identity.
 - **Audit:** use this page to view a log of all the changes that have been made to this identity.

Identities - Assigning Roles

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**.

The Identities Search page is displayed.


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

For more information, see *Searching for an Identity* on page 46.


3. Click on the name of the identity you want to edit.

The Identity Edit screen appears.

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  .

Identities - Assigning Tokens

Tokens allow users to have physical access to the system. Tokens can be a physical access card. 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.

To create tokens and assign them to an identity:

1. Click **Identities**.

The Identities Search page is displayed.

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

For more information, see *Searching for an Identity* on page 46.

3. Click on the name of the identity you want to edit.

The Identities Edit screen appears.

4. Select the **Tokens** tab.

5. If only one token has been defined, the Tokens Edit page appears.

If more than one token has been defined, the Tokens Listing page appears. Click **Add Token**.

6. Enter the details as required.

7. Click  .

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.

10. From the **Badge Token** drop down list, select the internal number you want to assign to the badge.

11. Click  (Save).

Identities - Assigning Groups

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**.

The Identities Search page is displayed.


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

For more information, see *Searching for an Identity* on page 46.


3. Click on the name of the identity you want to edit.

The Identities Edit screen is displayed.

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 .

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, 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 Internet Explorer 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 Internet Explorer web browser.

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.

NOTE: Images cannot be captured with a local camera from an ACM client running in the Internet Explorer or Safari web browsers, or running on a mobile device.
- **IP-based camera** — Any IP-based camera previously connected to your network and added to your ACM system.

NOTE: Images cannot be captured with a local camera from an ACM client running in the Internet Explorer or Safari web browsers, or running on a mobile device.


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 269.
- 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.

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.

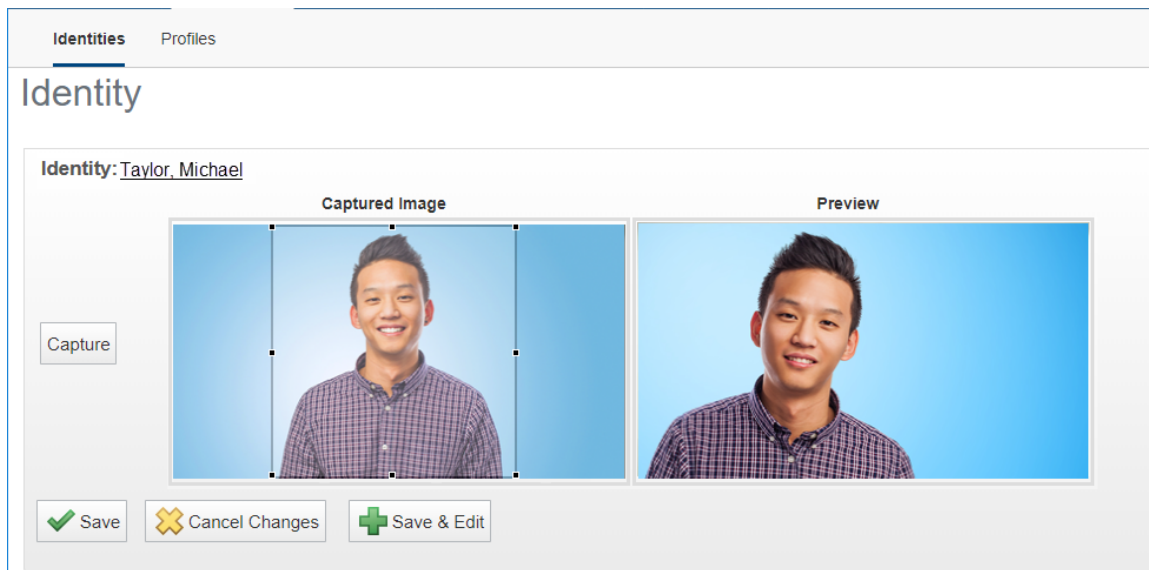
Enter a user name and password, then click **OK**.

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** check box if you want this photo to appear on this person's Identity page and access badge.

6. Click  .

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, GIF format.

3. On the **Photos** tab, click the **Primary** check box 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  .

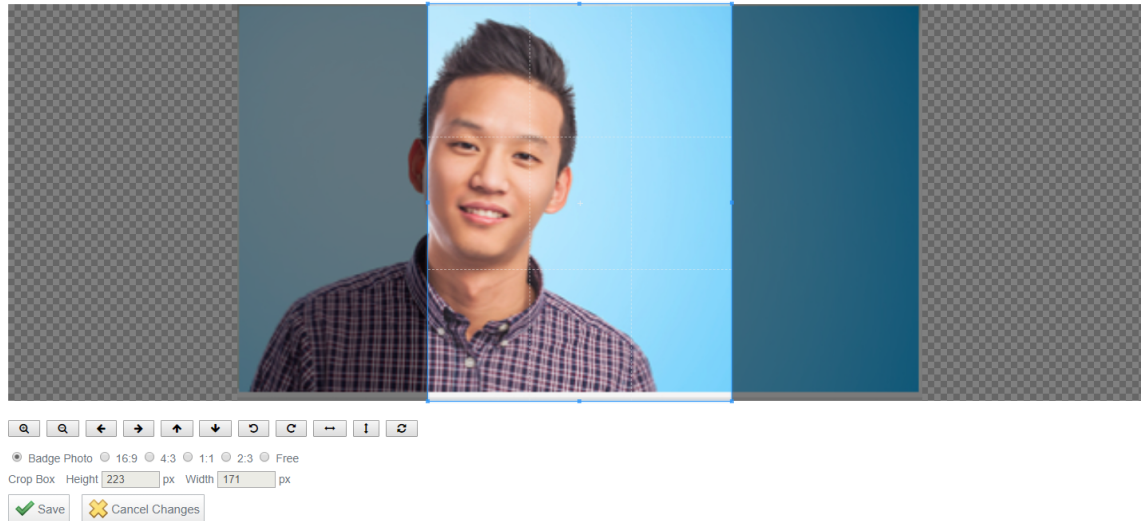
Editing a photo

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.

Photo Edit



1. Adjust the overlay.

- To reposition the overlay over the photo:
 1. Click inside the cropping overlay.
 2. Drag the mouse to move the overlay.
- To resize the overlay
 1. Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay can be resized.
 2. 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:
 1. Click **Free**.
 2. Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay will be resized.
 3. Drag the mouse to resize the overlay. The overlay will be resized only in the direction of the cursor.

- To rotate the overlay:
 1. Click outside the current overlay.
 2. Drag the mouse to draw a new overlay.
 - To replace the overlay:
 1. Click outside the current overlay.
 2. 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:
 1. Use the counterclockwise circular arrow to rotate the photo to the left by 90°.
 2. Use the clockwise circular arrow to rotate the photo to the right by 90°.
 - To flip the photo:
 1. Use the horizontal double-ended control button to flip the photo left to right..
 2. 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  .

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** check box of the photo you want.

Deleting a photo

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

1. Click  .
2. Click  .

Identities - Creating Badges

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**.

The Identities Listing page is displayed.

2. From the Identities Listing page, click on the name of the identity you want to edit.

The Identities Edit screen appears.

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 .

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**.
The Identities Search page appears.
2. Search for the identity. For more detail refer to *Searching for an Identity* on page 46.
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 newly added 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**.

The Identities Search page appears.

2. Search for the identity. For more information see *Searching for an Identity* on page 46.
3. Click on the name of the identity. The Identity: Edit page displays.
4. Click on the **Timed Access** tab.
5. Complete the following fields:
 - Name
 - Type
 - Appliance (this defaults)
 - Available/Members
 - Start Day/Time
 - End Day/Time
 - Schedule (if doors are selected as the Type)
6. Click **Add**.

The newly added timed access entry will display 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* above.


Deleting Timed Access

To delete a timed access entry:

1. Click **Identities**.

The Identities Search page appears.

2. Search for the identity. For more detail refer to *Searching for an Identity* on page 46.
3. Click on the name of the identity. The Identity: Edit page displays.
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.

The Identity Edit screen appears.

3. Navigate through the tabbed pages and make the required changes. The tabbed pages include:
 - **Identity:** use this page to edit the identity details.
 - **Roles:** use this page to assign a role to this identity.
 - **Tokens:** use this page to create a token for the identity.
 - **Groups:** use this page to assign this identity to a group.
 - **Capture:** use this page to take a photo of the user.
 - **Photos:** use this page to upload an existing photo of the user.
 - **Badge:** use this page to assign a badge to this user.
 - **Timed Access:** use this page to assign timed access to this user.
 - **Access:** use this page to view this identity's access privileges including roles, access groups, and doors.
 - **Transactions:** use this page to view past alarms and events that were triggered by this user.
 - **Audit:** use this page to view a log of all the changes that have been made to this identity.

NOTE: User Defined Tabs with User Defined Fields may be added. These will display at the end of the list.



NOTE: Remember to click  to save the changes on each page.

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.

Reports - 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 Listing page, 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 *Reports - Editing* 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.










Reports - Report Preview

When you click the name of a report from the Report Listing page 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.	
	<p>Click this icon to filter the report.</p> <p>The report filter options are displayed. The options change depending on the report.</p> <ul style="list-style-type: none"> • Click Search to perform a search using the selected filter options. • Click Reset to clear the report filter options. • 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. • 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.
Page <input type="text" value="1"/> of 1	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.


Reports - Editing


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 may want to create a custom report rather than modifying the default system report every time. For more information see *Reports - Creating Custom Reports* on page 62.

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 297.

1. Display the Reports Listing page.
 - To display the system reports page, click **Reports**.
 - To display the custom reports page, select **Reports > Custom Reports**.
2. Click  for the report that you want to edit.

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 - *Reports - Editing Audit Log and Transaction Reports* below.


3. On the following page, select your preferences for the report.
4. Click  to save your changes.

Now you can generate or preview the report with your changes.

Reports - 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 Listing page.

Follow the steps below to edit these reports.


1. Display the Reports Listing page.
 - 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 that you want to edit.
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. Panel Date).
 - 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

- Click  to add more search fields, if required.

Complete step 4 above for each additional field added.

- Click  **Save** to save your changes.

The ACM Notification message displays with the message 'Search Parameters successfully changed'.



- To save these filter settings as a custom report, enter a name in the Create Custom Report: field , then click  **Create Custom Report:.**

- To reset the search criteria, click  **Reset**

Now you can generate or preview the report with your changes.

Reports - 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 for filtered reports that are used frequently.


- Click **Reports**.
- Click  for the report you want to base the custom report on.
- On the following Report Edit page, select the **Copy Report** check box.
- Give the new report a name.
- Edit the report options to meet your requirements.
- Click  to save the new custom report.

The Custom Reports Listing page displays with the new report automatically added to the list.

Reports - 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.

The new report is automatically added to the Custom Reports Listing page.

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.

Configuring Templates (Mercury Security)

Defining panels, subpanels, and doors in the ACM system can take a long time due to the many options and attributes to configure. You can speed up the process by creating templates that can be used to create individual doors or to bulk create doors when adding Mercury panels:

- 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.

- Wiring templates

Standardize Mercury panels with wiring templates that link subpanel addresses to reader, input, and output templates. Wiring templates are used to batch create subpanels for doors when adding a Mercury panel.

- 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.

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 when adding a new panel, see *Batch Creating Subpanels on a New Mercury Panel* on page 87.
- 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 104.
- 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 Door Templates Listing page is displayed.

2. On the Door Templates Listing page, 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. 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 <i>Door Templates - Batch Update</i> on page 70.
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 Listing page, the Templates: Add page appears. Enter the required door template details.
- On the name of a door template on the Door Templates Listing page, 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 *User Lists - Adding Items to a List* on page 251.

Name the template and specify the site and vendor information.

Feature	
Name	Enter the name of the template.
Partitions	<p>If your site uses partitions, you can select the partitions for which this template is intended. The selection you make for the door template sets in which partitions doors are created.</p> <p>Click to select one partition, or use any of click and drag, Shift and click, or Ctrl and click to select multiple partitions.</p> <p>NOTE: In a partitioned system, operators can only see objects assigned to their assigned partitions, as well as any unpartitioned objects.</p>
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 149
- *Parameters tab (VertX®)* on page 135

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 152
- *Operations tab (VertX®)* on page 137

Door Templates - Edit page

When you click on the name of a door template on the Door Templates Listing page, 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.

NOTE: You can add additional values to some drop down lists using the User Lists feature. For more information, see *User Lists - Adding Items to a List* on page 251.

Name the template and specify the site and vendor information.

Feature	
Name	Enter the name of the template.
Partitions	<p>If your site uses partitions, you can select the partitions for which this template is intended. The selection you make for the door template sets in which partitions doors are created.</p> <p>Click to select one partition, or use any of click and drag, Shift and click, or Ctrl and click to select multiple partitions.</p> <p>NOTE: In a partitioned system, operators can only see objects assigned to their assigned partitions, as well as any unpartitioned objects.</p>
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 149
- *Parameters tab (VertX®)* on page 135

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 152
- *Operations tab (VertX®)* on page 137


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 Door Templates Listing page is displayed.

2. On the Door Templates Listing page, 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.

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 can 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.

Feature	Description
Name	The name of the reader template. 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.

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: <ul style="list-style-type: none">• OSDP

Feature	Description
	<p>Avigilon recommends using OSDP 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.</p> <ul style="list-style-type: none"> • F/2F. • D1/D0 (Wiegand) • CLK+Data (Mag) (NCI magnetic stripe standard) • Custom (Default) <p>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.</p>
The following options depend on the selected Reader Type and include:	
LED drive	<p>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:</p> <ul style="list-style-type: none"> • None • Gen 1 wire • Reserved • Sep Red/Grn no buzz • Dorado 780 • LCD • 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.
Keypad decode	<p>Select the keypad decode/encryption method that is used by readers configured with this template. The options include:</p> <ul style="list-style-type: none"> • MR20 8-bit tamper • Hughes ID 4-bit • Indala • MR20 8-bit no tamper
Wiegand	Check this box to indicate that readers configured with this template support the Wiegand standard.

Feature	Description
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	<p>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.</p> <p>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.</p>
Baud Rate	<p>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.</p> <p>NOTE: Mercury controllers will first try the setting provided and if that does not work, the controller will use default settings,</p>
OSDP Address	<p>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.</p> <p>NOTE: Mercury controllers will first try the setting provided and if that does not work, the controller will use default settings,</p>
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
VertX® settings	
Keypad decode	<p>Select the keypad decode/encryption method that is used by readers configured with this template. The options include:</p> <ul style="list-style-type: none"> • MR20 8-bit tamper • Hughes ID 4-bit • Indala • 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



Feature	Description
	standard for magnetic stripes.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
	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	
Reader Type	<p>Select the communication protocol used by readers configured with this template. The options include:</p> <ul style="list-style-type: none"> • OSDP <p>Avigilon recommends using OSDP 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.</p> • F/2F. • D1/D0 (Wiegand) • CLK+Data (Mag) (NCI magnetic stripe standard) • Custom (Default) <p>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.</p>
The following options depend on the selected Reader Type and include:	
LED drive	<p>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:</p> <ul style="list-style-type: none"> • None

Feature	Description
	<ul style="list-style-type: none"> • Gen 1 wire • Reserved • Sep Red/Grn no buzz • Dorado 780 • LCD • 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.
Keypad decode	<p>Select the keypad decode/encryption method that is used by readers configured with this template. The options include:</p> <ul style="list-style-type: none"> • MR20 8-bit tamper • Hughes ID 4-bit • Indala • 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	<p>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.</p> <p>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.</p>
Baud Rate	<p>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.</p> <p>NOTE: Mercury controllers will first try the setting provided and if that does not work, the</p>

Feature	Description
	controller will use default settings,
OSDP Address	<p>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.</p> <p>NOTE: Mercury controllers will first try the setting provided and if that does not work, the controller will use default settings,</p>
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
VertX® settings	
Keypad decode	<p>Select the keypad decode/encryption method that is used by readers configured with this template. The options include:</p> <ul style="list-style-type: none"> • MR20 8-bit tamper • Hughes ID 4-bit • Indala • 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	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
	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 can 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. Click the name to edit the input template details.
Delete	Click  to delete the input template.
	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. <ul style="list-style-type: none">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.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

Feature	Description
	<p>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.</p> <ul style="list-style-type: none"> 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	<p>Select the End of Line resistance value used by inputs configured with this template.</p> <p>Only the EOL resistance values that have been defined in the system are listed.</p>
Debounce¹	Select how often the unit is allowed to debounce in a row. 1 = 16 ms, 2 = 32 ms, etc.
Entry Delay	<p>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.</p> <p>Enter the number of seconds allowed before the input reports an event.</p>
Exit Delay	<p>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.</p> <p>Enter the number of seconds allowed before the input reports an event.</p>
Hold time	<p>Set the amount of time that the alarm will stay in alarm state after returning to normal.</p> <p>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.</p>
Schedule	<p>Define when the input is masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Masked	Check this box to indicate that this input is normally masked.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>

¹Due 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 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

Mode	<p>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.</p> <ul style="list-style-type: none"> • 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. • 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. • 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	<p>Select the End of Line resistance value used by inputs configured with this template.</p> <p>Only the EOL resistance values that have been defined in the system are listed.</p>

Feature	Description
Debounce¹	Select how often the unit is allowed to debounce in a row. 1 = 16 ms, 2 = 32 ms, etc.
Entry Delay	<p>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.</p> <p>Enter the number of seconds allowed before the input reports an event.</p>
Exit Delay	<p>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.</p> <p>Enter the number of seconds allowed before the input reports an event.</p>
Hold time	<p>Set the amount of time that the alarm will stay in alarm state after returning to normal.</p> <p>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.</p>
Schedule	<p>Define when the input is masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Masked	Check this box to indicate that this input is normally masked.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
	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.

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.

¹Due 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".



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 can 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. 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 .
Operating Mode	Select how the panel knows when the output point is active. <ul style="list-style-type: none"> • Energized When Active – a current is expected to pass through the output point when it is <i>active</i>. • Not Energized When Active – a current expected to pass through the output point when it is <i>inactive</i>.
Pulse Time	Enter the pulse interval time. This is the number of seconds that the output will activate when a pulse command is issued. NOTE: This field is only available on outputs not associated with doors (e.g. auxiliary relays).
Schedule	Define when this output is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Partitions	NOTE: If no partitions are defined for this system, this feature is not available.


Feature	Description
	<p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
	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	<p>Select how the panel knows when the output point is active.</p> <ul style="list-style-type: none"> • Energized When Active – a current is expected to pass through the output point when it is <i>active</i>. • Not Energized When Active – a current expected to pass through the output point when it is <i>inactive</i>.
Pulse Time	<p>Enter the pulse interval time. This is the number of seconds that the output will activate when a pulse command is issued.</p> <p>NOTE: This field is only available on outputs not associated with doors (e.g. auxiliary relays).</p>
Schedule	<p>Define when this output is active.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
	Click this button to save your changes.

Feature	Description
	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 doors in the ACM appliance. A wiring template corresponds to a standard wiring setup for the doors connected to a specific Mercury subpanel model. Create a wiring template for each type of subpanel in use at your site. If you use different wiring setups for the same type of subpanel, you can 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. 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 required wiring template details.




Feature	Description				
Name	Enter a unique name for the template.				
Vendor	The only option is Mercury Security .				
Model	Select from the drop-down list:				
	<table><tr><th>Model</th><th>Number of Doors</th></tr><tr><td>One door module</td><td>1</td></tr></table>	Model	Number of Doors	One door module	1
	Model	Number of Doors			
One door module	1				

Feature	Description	
	Model	Number of Doors
	Two door module	2
	1502 Internal SIO	2
	51e	2
	1501 Internal SIO	1
	M5-2RP	2
	M5-2SRP	2
	M5-8RP	8
	MS-2K	4
	MS-ACS	8
For each door:		
Door	Select	Select
	Reader Address	Reader Template
	Alt Reader Address	Reader Template
	Door Position Address	Input Template
	Strike	Output Template
	REX 1	Input Template
	REX 2	Input Template
	Click to save the template and return to the Wiring Templates list page.	
	Click to return to the Wiring Templates list page without saving.	
	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 appears. Modify the required wiring template details.

Feature	Description
Name	Enter a unique name for the template.
Vendor	The only option is Mercury Security .
Model	Select from the drop-down list:

Feature	Description	
	Model	Number of Doors
	One door module	1
	Two door module	2
	1502 Internal SIO	2
	51e	2
	1501 Internal SIO	1
	M5-2RP	2
	M5-2SRP	2
	M5-8RP	8
	MS-2K	4
	MS-ACS	8
For each door:		
Door	Select	Select
	Reader Address	Reader Template
	Alt Reader Address	Reader Template
	Door Position Address	Input Template
	Strike	Output Template
	REX 1	Input Template
	REX 2	Input Template
	Click to save the template and return to the Wiring Templates list page.	
	Click to return to the Wiring Templates list page without saving.	
	Click to add a new wiring template.	

Configuring Panels

Panels are controllers that connect one or more door controllers (subpanels) and their associated readers to the 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 panel is created you can batch add subpanels and door subpanels and create the doors connected to each door subpanel. You must configure door templates, wiring templates, input templates, and output templates before you can batch subpanels for doors. 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 *Configuring Templates (Mercury Security)* on page 64

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**.

Adding Panels

Panels connect door controllers and their readers to the appliance. Adding a panel to the ACM system allows the appliance to gather information on the connected doors.

To add a panel to the system:

1. Select **Physical Access > Panels**.
The Panels Listing page is displayed.
2. Click **Add Panel**.
The Panel Add page is displayed.
3. Enter a unique **Name** for the panel, and optionally identify its **Physical Location**.
4. Complete the **Vendor** and **Model** fields. Depending on the selected Vendor and Model, different options are displayed.
5. When you're finished, click  to save your changes:
 - Mercury panels: The first page of the Subpanel: Batch Create wizard for the new panel is displayed. For more information, see *Batch Creating Subpanels on a New Mercury Panel* on the next page.

Important: PIM400, ENGAGE™ Gateway, and AD300 subpanels cannot be batch added to a Mercury panel. You must add them using the procedure below. If you are connecting these subpanels you cannot add any other subpanel models to the same port. For more information, see *Adding a Subpanel* on page 95.

- VertX® panels: the Subpanel: Batch Add page (VertX®) for the new panel appears.

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 Access Control Manager system.


For more information, see *Adding Panels* on the previous page.

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 90.

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 104.

5. Customize the door settings to meet your system requirements and save your changes.

Batch Creating Subpanels on a New Mercury Panel

After saving a new Mercury panel, you can batch create the subpanels and doors connected to the new Mercury panel using the Subpanel: Batch Create wizard, up to the maximum supported by the panel.

Create templates for doors, readers, outputs, and inputs, and a templates for wiring panels. The more you standardize doors, readers, outputs, inputs, and panel wiring, the fewer templates are required. The wizard creates functional subpanels and doors with the information from the templates. For more information, see *Configuring Templates (Mercury Security)* on page 64.

Without templates specified, the wizard creates blank objects you can individually configure later.

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: PIM400, ENGAGE™ Gateway, and AD300 subpanels must be added one at a time.

In the wizard, entering subpanel information is a three-step procedure:

1. Add the subpanels to create, defining a base name for the subpanels, the quantity, and the templates to use. When you add a door model and specify a door template and a wiring template, the subpanels and doors are automatically created with the settings in both templates in the third step.
2. Edit the default subpanel addresses and the subpanel names.
3. Review your configuration entries, and edit the default door names for any door subpanels, before the subpanels are created.

Each step is completed on its own page. The subpanels are not created until you 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.

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 not created until you save after completing the third step.



Tip: After you have configured new doors using templates, you can access each door, panel, or subpanel to configure the unique settings that are not configured by each template.

Subpanel: Batch Create page (Mercury Security)

Add a row for each differently configured subpanel connected to the new 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.

An exception to this is the MS-ISC panel, which only supports addresses 0 and 2 for MS-ACS subpanels. You can add more than two MS-ACS subpanels to an MS-ISC panel on the first page, but when you proceed from the second page (Subpanel: Batch Edit Details) to the third page (Subpanel: Batch Name Doors), you will be prompted to correct this.



Feature	Description
Subpanel Type	<p>For each row, select a module type from the Select Model drop-down list. After you make your selection, the row is updated to prompt you for the information needed to create the subpanel.</p> <p>There are three categories of subpanels that can be created:</p> <ul style="list-style-type: none"> • Door subpanels • Input subpanels • Output subpanels
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 subpanels you want to add. The number of available subpanels is updated as new rows are added.
Template	Two columns to specify the templates you want the wizard to use to create the subpanels. The first column is for the door template and the input template. The second column is for the wiring template and the output template. The columns change based on the type of subpanel chosen, on per-row basis:

Feature	Description
	<ul style="list-style-type: none"> • A functional subpanel for a door needs a door template and a wiring template. • An unconfigured subpanel for a door needs a door template. • A functional input template uses an input template. • A functional output subpanel uses an output template. <p>Templates are not required to create unconfigured subpanels.</p>
	Click this button to add a row.
	Click this button to delete a row.

Click **Next** and the **Subpanel: Batch Edit Details** page is displayed.

Subpanel: Batch Edit Details page (Mercury Security)

Edit the details for all of the subpanels you defined for the new panel. You can also add subpanels up to the maximum supported by the panel.

Feature	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.
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 actual name of each subpanel. The default name is the subpanel address appended to the Subpanel Base Name from the previous page: <panelName>-<panelModel>-<subpanelAddress>. For example EastEntrance-LP2500-0. You can change this name.
Template	Two columns to specify the templates you want the wizard to use to create the subpanels. The same guidelines used on the previous page apply here.
	Click this button to add a row.
	Click this button to delete a row.

Click **Next**.

- The Subpanel: Batch Name Doors page is displayed if you are configuring door subpanels and specified door templates to use.
- The Subpanel: Batch Create Summary page is displayed if you are configuring input or output subpanels, or door subpanels without specifying any door templates.

Subpanel: Batch Name Doors or Subpanel: Batch Create Summary page (Mercury Security)

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. This page appears if you have specified door subpanels and door templates on the previous pages.

On the Subpanel: Batch Create Summary page the settings you have configured on the previous pages are displayed for your review before the subpanels are created. This page appears if you are configuring subpanels without using any door templates.



Feature	Description
Address	Display only.
Subpanel Type	Display only.
Subpanel Name	Display only.
Template	Display only.
Door Name	If you have specified a door template for a door, the default name is displayed. The default format is <panelName>-<panelModel>-<Address>-door<n>. For example EastEntrance-LP2500-2-door0. You can change this name.

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 Subpanels: 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 .

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.

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 Listing page, 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 Listing page, 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 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.
- **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.

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 Listing page, 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. Cardholders 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 Listing page, 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 Listing page, 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

Access Control Manager 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
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 Access Control Manager appliance can communicate with the panels in the same way.

Resetting Doors/Subpanels

To reset all the doors that are connected to a specific panel:

1. Click **Physical Access** > Panels to open the Panels list.
2. On the Panels list, click the panel you want to reset to open the **Panel: Status** page.
3. Click the **Reset/Download** button.

All the subpanels that are connected to the panel are reset and the latest configurations from the Access Control Manager system are downloaded. Doors connected to this panel are now updated with the most recent configuration.

Updating Panel Firmware



When you get an update to the panel software, use the ACM system to apply the update. The firmware is downloaded to the panel and the panel is reset. The reset activates the new firmware, and downloads and applies the latest ACM system configuration parameters for the panel.


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.



Panel firmware is usually downloaded from the panel manufacturer.

1. On the Panels Listing page, select the panel you want to update.
2. On the Panel Status page, click **Firmware**.

The Firmware Listing page is displayed.

3. Perform any of the following:
 - To apply a firmware update that is already available in the system, click  beside the firmware update file.
 - To add and apply a new firmware update file provided by the panel manufacturer:
 - a. Click **Add Firmware**.
 - b. On the following Firmware Upload page, click **Choose File** then locate the firmware file.
 - c. Click  to upload the new firmware to the system.

NOTE: If you click , the **Identity Import Type:** will be set to **Auto** and any attached CSV files will be deleted.

 - d. On the Firmware Listing page, click  beside the new firmware update to apply it to the panel.
 - To delete an existing firmware update file, click  beside the firmware file. When the confirmation message is displayed, click **OK**.

Updating Panel Time

Each panel typically tells time by synchronizing with a time server (NTP Server) that is accessible on the network. In the event of an unexpected power or network failure, the panel may be running independently for a while and will need to be re-synchronized when everything is back online.

NOTE: Not all panels support this feature. This procedure can only be performed if the panel status page displays the **Clock** button.

1. On the Panels Listing page, select the panel you want to update.
2. On the Panel Status page, click **Clock**.

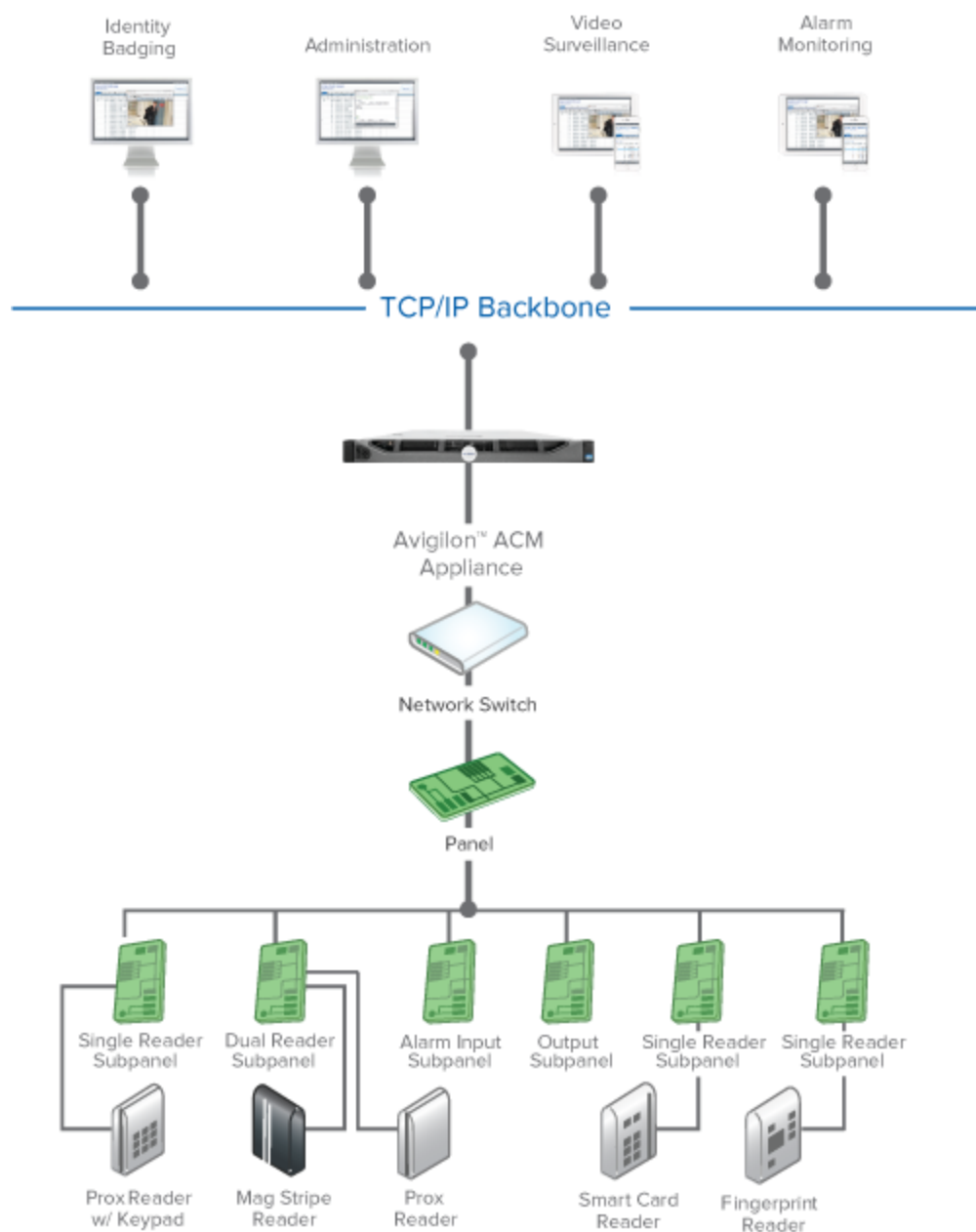
The panel connects and synchronizes with a time server that is accessible on the network.

Deleting Panels

1. From the Panels Listing page, click  for the panel you want to remove.
2. 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 panel any time after the panel has been added to the ACM system. PIM400, ENGAGE™ Gateway, and AD300 subpanels can only be added one at a time. Use this procedure to add single subpanels to a panel.


You can use the Subpanel: Batch Create wizard only when a panel is first added to the ACM system to batch add subpanels to a panel. For more information about batch adding subpanels, see:

- *Adding Panels* on page 86
- *Batch Creating Subpanels on a New Mercury Panel* on page 87

Tip: Create door templates, wiring templates, reader templates, output templates, and input templates for the Subpanel: Batch Create wizard to use to create functional subpanels for doors, inputs, outputs, or readers. For more information, see *Configuring Templates (Mercury Security)* on page 64.





- Panels - Subpanel: Batch Add page (VertX®)

To add subpanels one at a time from the Panel screen:

1. Select **Physical Access > Panels**.
2. Click the name of the panel that the new subpanel is physically connected to.
3. Select the **Subpanels** tab.
4. Click **Add New Subpanel**.
5. Complete the details for the new subpanel.
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 Listing page, 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.
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 101 and *Configuring Panels* on page 85.

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 stop a panel from communicating to a subpanel, you can delete it from the system.

1. Select **Physical Access > Panels**.
2. Click the name of the panel the subpanel is connected to.
3. Select the **Subpanels** tab.
4. Click  for the subpanel you want to remove from the system.
5. When the confirmation message appears, click **OK**.

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, unmask the alarms, locks all the doors connected to a panel, turns out the lights, then emails the operator for more instructions.

In the Avigilon Access Control Manager 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 106.


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 New Macro**.
4. On the following Macro Command Listing page, 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 New 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* below.

To create quick macros that are specific to a particular door (simple macros), see *Adding Simple Macros* on page 106.

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
4. On the following Macro Command Listing page, 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 New 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 106 and *Operations tab (Mercury Security)* on page 152.

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 Listing page, 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/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 *Configuring Templates (Mercury Security)* on page 64. For more information about the Subpanel: Batch Create wizard, see *Batch Creating Subpanels on a New Mercury Panel* on page 87.

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 Listing page.

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 Listing page refreshes to show the doors that meet your filters.

Controlling Doors

From a Doors listing page, you can use the options on the Door Action, Door Mode, Forced, Held, and Installed drop-down menus to control doors. For example, you can choose a door and unlock it to allow unrestricted access to an area.

Doors can also be controlled from a map monitoring page. For more information, see *Using a Map* on page 279.

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

1. Select the check box beside the door you want to control.

If you want to affect all the doors in your system, click **All** at the top of the left column to select all the doors.

2. Select any of the following Door Actions if required:

- **Grant** — Click this button to grant temporary access to the specified door. The door will be momentarily unlocked to permit entry through the door.
- **Restore** — Click this button to restore the door to its default configuration values. Restoring a Door that has an activated Lock Function (Classroom, Office, Privacy, or Apartment), will remove the Lock Function and the door will be reset to its default configuration.


- **Unlock** — Click this button to unlock the specified door. This door will remain unlocked until the **Locked No Access** command is issued or until another change of state is directed (either via operator override or scheduled action).
 - **Locked No Access** — Click this button to lock the specified door. This door will remain locked until the **Restore** command is issued or until another change of state is directed (either via operator override or scheduled action).
 - **Disable** — Click this button to disable the specified door. This door will stop operating and allow no access.
3. Select any of the following Door Mode options to change the door mode:
 - **Card Only** — This door can be accessed using a card. No PIN 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.
 - **Pin Only** — This door can only be accessed by entering a PIN at a keypad. No card is required.
 - **Facility Code Only** — This door can be accessed using a facility code.
- NOTE:** The Pin only and Card or Pin door modes will not be available if the 'Allow duplicate PINs' option has been selected on the System Settings - General page.
4. Select either of the following Forced options if required:
 - **Mask Forced** — Click this button to mask the Forced Door Alarm for this door.
 - **Unmask Forced** — Click this button to unmask the Forced Door Alarm for this door.
 5. Select either of the following Held options if required:
 - **Mask Held** — Click this button to mask the Door Held Open Alarm for this door.
 - **Unmask Held** — Click this button to unmask the Door Held Open Alarm for this door.
 6. Select either of the following Installed options if required:
 - **Install** — Click this button to install a door.
 - **Uninstall** — Click this button to uninstall a door.

Adding Doors

To add a new door:

1. Select **Physical Access**.
The Door Listing page is displayed.
2. On the Door Listing page, click **Add Door**.
Using a Door Template (Mercury Security only)

If door templates are configured at your site, the Templates dialog appears. A door template is used to automatically populate field values on the Parameters and Operations tabs of the new door.

- To use the door settings from a template:
 1. Select the template and click **OK**. When a template is selected the screen immediately refreshes and settings from the template are applied.
 2. Enter the **Name** of the new door.
 3. Specify the **Panel** (if more than one panel is available), **Subpanel** (if more than one subpanel is available), and **Lock Number/Door Number** (for a wireless lock only).
 4. Click  .

The new door is added. You can now configure the door-specific settings on the other tabs that are now displayed.

NOTE: There are no template settings for Avigilon doors, which enable the ACM Verify feature.

- Otherwise, click **Cancel** in the Templates dialog and manually enter all the settings for the new door.

For information about door templates, see *Configuring Templates (Mercury Security)* on page 64

3. On the Door Add page, enter a name for the door.

NOTE: Complete the **Alt Name** field if required.

4. From the **Appliance** drop down list, select the related appliance.
5. From the **Vendor** drop down list, select the manufacturer of the panel that controls the door.

NOTE: Depending on the vendor selected, additional fields will display.

6. Click  to add the door.

NOTE: Once saved the page becomes the Door: Edit page.

7. Navigate through the tabbed pages to configure the door. The tabbed pages include:
 - **Parameters:** Use this page to set access type, processing attributes, and other options.
 - **Operations:** Use this page to set simple macros, accepted card formats, and other options.
 - **Hardware:** Use this page to set reader, door position, strike and request to exit (REX).
 - **Elev:** Use this page to view elevator door details.
 - **Cameras:** Use this page to add or remove associated cameras.
 - **Interlocks:** Use this page to set interlocks.
 - **Events:** Use this page to view and edit door events.
 - **Access:** Use this page to view access groups, roles and identities that have door access.
 - **Transactions:** Use this page to view door transactions.

8. 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 98.

1. Select **Physical Access**.

The Door Listing page is displayed.

2. Select a door from the Door Listing page.
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**.

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.

For definitions of the relevant fields and pages for each door type, refer to the page specific to your door vendor.

3. Edit the details on each tab as required:

- **Parameters:** Use this page to set access type, processing attributes, and other options.
- **Operations:** (Mercury Security and VertX® only) Use this page to set simple macros, accepted card formats, and other options.
- **Hardware:** (Mercury Security and VertX® only) Use this page to set reader, door position, strike and request to exit (REX).
- **Elev:** (Mercury Security only) Use this page to view elevator door details.
- **Cameras:** Use this page to add or remove associated cameras.
- **Interlocks:** (Mercury Security only) Use this page to set interlocks.
- **Events:** Use this page to view and edit door events.
- **Access:** Use this page to view access groups, roles and identities that have door access.
- **Transactions:** Use this page to view door transactions.

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 page 135
- *Door: Edit page (Mercury Security)* on page 149

4. After editing each tab, click  to save your changes.

Doors - Editing VertX® Doors


1. Select **Physical Access**.

The Doors Listing page is displayed.

2. From the Doors Listing page, click the VertX® door name you want to edit.

The Doors Edit screen for that specific door type is displayed.

3. Edit the door by changing values on each of the door option tabs.

4. When you're finished, click .

You are returned to the Listing page 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. When you're finished, click .

You are returned to the Listing page with all changes saved.

Deleting Doors

To delete a door:

1. From the Door Listing page, 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.

Door Modes

When you see the Door Mode option on the Door Edit page, the following options are listed:

This same list of options is provided for the Offline Door Mode option.

NOTE: Some of the options are not listed if it is not supported by the door module.

Feature	Description
Disable	This door is disabled for all access.
Locked no access	This door is always locked. No access is allowed through this system.
Facility code only	This door can be accessed using a facility code. 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.
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: This door mode is not available if the 'Allow duplicate PINs' option has been selected on the System Settings - General page.
Card and Pin	This door can only be accessed using both a card and a PIN.
Card only	This door can be accessed using a card. (The type of reader used to read this card is determined in the Reader Type field.) No PIN is required.
Pin only	This door can only be accessed by entering a PIN at a keypad. No card is required. NOTE: This door mode is not available if the 'Allow duplicate PINs' option has been selected on the System Settings - General page.
Unlocked	This door is always unlocked.

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 Master	<p>This indicates that this door possesses a reader/keypad on both sides, entry and exit, and that this side is the master.</p> <p>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.</p>
Paired Slave	<p>This indicates that this door possesses a reader/keypad on both sides, entry and exit, and that this side is the slave.</p> <p>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.</p>
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 cardholder enters a room then passes the card to another potential cardholder to reuse the card at the same door, an APB error is logged and may be configured to prevent the second cardholder from entering.

Another example is when an access card is also required to exit. If a cardholder 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 cardholder 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 for **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.
Door-Based	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

Mode	Description
Timed APB	<p>reached.</p> <p>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.</p> <p>NOTE: This mode is only available if using Mercury Security hardware.</p>
Token-Based Timed APB	<p>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.</p> <p>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.</p> <p>NOTE: This mode is only available if using Mercury Security hardware.</p>
Hard Door APB	<p>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.</p> <p>Enter a value in the APB Delay field to create a time-based APB.</p> <p>NOTE: This mode is only available if using VertX® hardware.</p>
Soft Door APB	<p>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.</p> <p>Enter a value in the APB Delay field to create a time-based APB.</p> <p>NOTE: This mode is only available if using VertX® hardware.</p>
Hard Area APB	<p>Tracks each badge that enters a specific area and defines which areas the badge may access next. This badge is denied access if it tries to access an undefined area.</p> <p>Enter a value in the APB Delay field to create a time-based APB.</p> <p>Make sure you configure the area entering and area leaving setting for the specified door.</p>
Soft Area APB	<p>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.</p> <p>Enter a value in the APB Delay field to create a time-based APB.</p> <p>Make sure you configure the area entering and area leaving setting for the specified door.</p>
Timed Area APB	<p>Time based hard area APB. When the time limit expires, the hard area APB becomes a soft area APB.</p> <p>Make sure you configure the area entering and area leaving setting for the specified door.</p> <p>NOTE: This mode is only available if using Mercury Security hardware.</p>

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 the previous page.

To use the APB feature, you must set up at least two doors: one to represent the entrance and one to represent an exit.

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 Master** 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 Slave** as the Access Type. This door will only control the reader that allows cardholders 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.

NOTE: 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.

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 cardholder 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 Listing page is displayed.
2. From the Identities Listing page, 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 cardholder can now enter the door without generating an new anti-passback alarm.

Global Anti-Passback

The anti-passback (APB) feature is used when you want to identify every cardholder that enters a room or area. This feature can be configured to log or prevent a cardholder from re-entering the same area unexpectedly.

For example, the same card cannot be used to enter the same room twice in a row. If a cardholder enters a room then passes the card to another potential cardholder to reuse the card at the same door, an APB error is logged and may be configured to prevent the second cardholder from entering.

Another example is when an access card is also required to exit. If a cardholder 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 cardholder to log an entrance in the system before they can exit.

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 user violation, it will prevent that user from entering through other doors in same area.

Global Anti-Passback Modes

When you select the **Operations** tab on the Door Edit page, one of the options is for **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.

NOTE: The APB modes may be different depending on the panels you have installed.

Tip: For VertX® panel controlled doors, enter a value in the **APB delay** field to create a time based APB.

Mode	Description
No Selection	APB is not used.
Door-Based Timed APB	<p>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.</p> <p>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.</p> <p>NOTE: This mode is only available if using Mercury Security hardware.</p>

Mode	Description
Token-Based Timed APB	<p>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.</p> <p>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.</p> <p>NOTE: This mode is only available if using Mercury Security hardware.</p>
Hard Door APB	<p>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.</p> <p>Enter a value in the APB Delay field to create a time-based APB.</p> <p>NOTE: This mode is only available if using VertX® hardware.</p>
Soft Door APB	<p>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.</p> <p>Enter a value in the APB Delay field to create a time-based APB.</p> <p>NOTE: This mode is only available if using VertX® hardware.</p>
Hard Area APB	<p>Tracks each badge that enters a specific area and defines which areas the badge may access next. This badge is denied access if it tries to access an undefined area.</p> <p>Enter a value in the APB Delay field to create a time-based APB.</p> <p>Make sure you configure the area entering and area leaving setting for the specified door.</p>
Soft Area APB	<p>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.</p> <p>Enter a value in the APB Delay field to create a time-based APB.</p> <p>Make sure you configure the area entering and area leaving setting for the specified door.</p>
Timed Area APB	<p>Time based hard area APB. When the time limit expires, the hard area APB becomes a soft area APB.</p> <p>Make sure you configure the area entering and area leaving setting for the specified door.</p> <p>NOTE: This mode is only available if using Mercury Security hardware.</p>

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 Listing page 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 Listing page is displayed.

Accessing Interlocks from Subpanel Inputs

1. Select **Physical Access>Panels**.

The Panels Listing page is displayed.

2. Select the panel you want to interlock.

The Panel Status screen is displayed.

3. Click the **Subpanels** tab.

The Subpanels Listing page is displayed.

4. Click  for the subpanel that is connected to the input you want to interlock.

The Inputs Listing page is displayed.

5. Click the **Interlocks** link beside the required input.

The Input Interlock Listing page is displayed.

Accessing Interlocks from Subpanel Outputs

1. Select **Physical Access>Panels**.

The Panels Listing page is displayed.

2. Select the panel you want to interlock.

The Panel Status screen is displayed.

3. Click the **Subpanels** tab.

The Subpanels Listing page is displayed.

4. Click  for the subpanel that is connected to the output you want to interlock.

The Outputs Listing page is displayed.

5. Click the **Interlocks** link beside the required output.

The Output Interlock Listing page is displayed.


Adding Interlocks

1. From the Interlock Listing page, click **Add New Interlock**. For more information about how to access the different Interlock Listing pages, see *Interlocks* on page 113.
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 Listing page, click the name of an interlock. For more information about how to access the different Interlock Listing pages, see *Interlocks* on page 113.
2. On the following Interlock Edit page, make the required changes.
3. Click  to save your changes.

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.

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 EP1501, EP1501 with downstream support, EP1502 or EP2500
- Assa Abloy Aperio 1 to 8 Hub or 1 to 1 Hub

The wireless lock assembly is installed directly to the door and communicate with the Aperio Hub subpanel wirelessly.

1. Add a Mercury EP1501 or EP2500 panel to the Access Control Manager system.
For more information, see *Adding Panels* on page 86.
2. Add the **Aperio 1 to 8 Hub** or **Aperio 1 to 1 Hub** as a subpanel to the panel added in the previous step.
For more information, see *Adding Mercury Security Panels* on page 90.
For more information, see *Adding Mercury Security Panels* on page 90.
3. Create a door for each wireless lock assembly.
For more information, see *Adding Doors* on page 104.
4. For each door, select the corresponding Mercury Security panel, Aperio Hub subpanel and Lock Number that is assigned to the wireless lock assembly.
5. Customize all other door settings to meet your system requirements and save your changes.

Configuring Allegion Schlage AD400 Series Locks

To use Allegion Schlage AD400 series locks, you must have the following panels connected to the system:

- Mercury EP1501 or EP2500 panel with downstream support
- PIM400 subpanel that is wired to the Mercury panel

The wireless lock assembly is installed directly to the door and communicates with the PIM400 subpanel wirelessly.

NOTE: Ensure that the wireless locks have been installed in line with Schlage's installation instructions.

1. Add a Mercury EP1501 or EP2500 panel to the Access Control Manager system.

For more information, see *Adding Panels* on page 86.

2. Add the PIM400 as a subpanel to the panel in the previous step.

For more information, see *Adding Mercury Security Panels* on page 90.

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 104.

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 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.
- **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.
- **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: 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.




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 the following panels connected to the system:

- Mercury EP1501 or EP2500 panel with downstream support.
- ENGAGE™ Gateway subpanel that is wired to the Mercury 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 Access Control Manager system following the steps below:
 - Select **Physical Access > Panels** to open the Panels page.
 - Click  to add a new panel on the Panel: Add New page.
 - Enter the Name, Vendor (Mercury Security), Model (2500 or 1501 with Downstream) and select **Installed**, then click  to save the new panel.
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 90.

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 LE 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 104.

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. The options are:
 - **None** — Use the system default door settings.
 - **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.
 - **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.
 - **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: 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 Allegion Schlage NDE Series Locks

To use Allegion Schlage NDE series locks, you must have 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 Access Control Manager system following the steps below:
 - Select **Physical Access > Panels** to open the Panels page.
 - Click  to add a new panel on the Panel: Add New page.
 - Enter the Name, Vendor (Mercury Security), Model (2500 or 1501 with Downstream) and select **Installed**, then click  to save the new panel.
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 90.

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 104.
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.

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 configured in the format `MAC<nnnnnnnnnn>`, where `nnnnnnnnnn` 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).

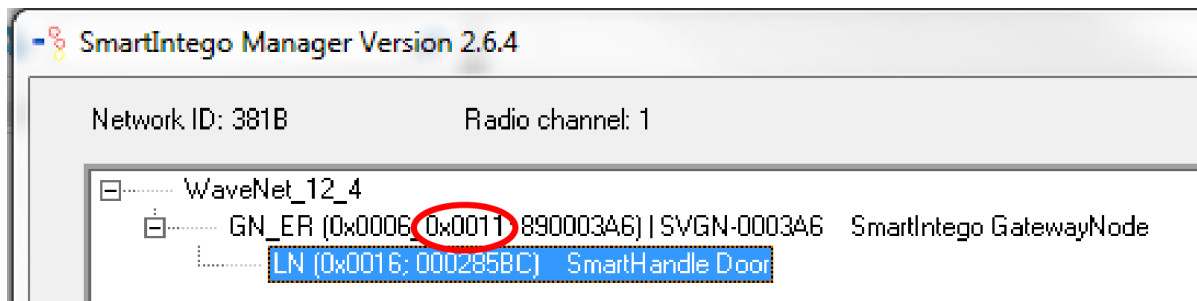


Figure 3: The SmartIntego GatewayNode hexadecimal address in the SmartIntego Manager screen of the SmartIntego Tool.

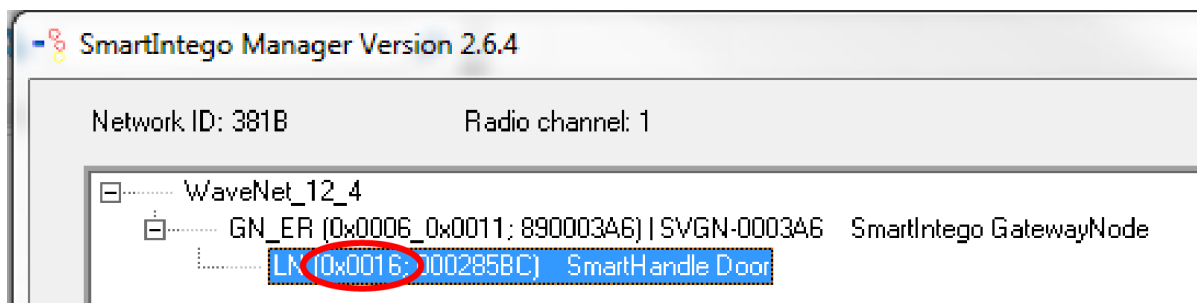





Figure 4: The SmartIntego lock hexadecimal address in the SmartIntego Manager screen of the SmartIntego Tool.

NOTE: The SmartIntego Tool software and the SmartIntego GatewayNode software are not supported on Microsoft Windows 10.

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 Access Control Manager system following the steps below:
 - Select **Physical Access > Panels** to open the Panels page.
 - Click  to add a new panel on the Panel: Add New page.
 - Enter the Name, Vendor (Mercury Security), Model (one of the supported panels) and select **Installed**, then click  to save the new panel.
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 104.
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. 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.

After the door is operational:

- 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 polling time can be variable.

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.

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.

NOTE: 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 page 104 and *Door: Add page* on the next page
- Select doors in the list and click the **Delete** control button.

Editing doors and panels:

- Click the link to the door in the **Name** column. For more information, see *Editing Doors* on page 106.
- 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 103.

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	<p>Displays the device status. Hover the mouse over the related icon to see more details.</p> <p>NOTE: The tamper icon only appears for OSDP readers, and reports whether the reader is offline or has been tampered with.</p>
Name	<p>The name assigned to this door.</p> <p>Click on this name to open the Door: Edit page Parameters tab .</p>
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	<p>Current state of the related door: Open or Closed.</p> <p>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.</p>
Door mode	<p>Indicates the door mode — the method by which the door is opened:</p> <ul style="list-style-type: none"> • Disabled • Unlocked • Locked No Access • Facility Code Only • Card Only • Pin Only • Card & Pin • Card or Pin



Door: Add page

When you click **Add Door** from the Doors Listing page, the Door: Add page is displayed.

Important: If door templates are used, the Templates dialog appears. To use the door settings from a template, select the template and click OK. Otherwise, click Cancel.

NOTE: Fields in this list that are not supported by the door module may not be displayed.

Feature	Description
Name	Enter a name for the door.
Alt. Name	If required, enter an alternate name for the door.
Location	Enter a short description of the door location.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	<p>Specifies the panel the door is assigned to.</p> <p>After you make your selection, new options may be displayed to define how the door is connected to the panel:</p>
	<p>Subpanel Specifies the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the selected main panel.</p>
	<p>Specifies a configured group of readers, inputs, and outputs that are connected from the subpanel to the door.</p> <p>For wired connections, select the door number from the drop-down list.</p> <p>Lock Number For wireless locks only: or Door Number</p> <ul style="list-style-type: none"> • Enter the number programmed for the lock. For all locks except SimonsVoss, select the number from the drop-down list. • For SimonsVoss wireless locks, enter the hexadecimal address assigned by the SmartIntego Tool. For more information, see <i>Configuring SimonsVoss Wireless Locks</i> on page 119.
Appliance	Select the ACM appliance that the door is connected to.
Vendor	<p>Select the type of panel this door is connected to.</p> <p>The page refreshes to display new options:</p> <ul style="list-style-type: none"> • If you are adding an Avigilon Door, see <i>Options for an Avigilon Door</i> on the next page • If you are adding an VertX® door see <i>Options For VertX® and Mercury Security Doors</i> on the next page and <i>Door Processing Attributes for VertX® Doors</i> on page 128 • If you are adding a Mercury Security door, see <i>Options For VertX® and Mercury Security Doors</i> on the next page and <i>Door Processing Attributes for Mercury Security</i>

Feature	Description
	<i>Doors on page 129.</i>
Installed	Check this box to indicate that all the door components are installed and can communicate with the appliance.
	Click this button to save your changes.
	Click this button to discard your changes.

Options for an Avigilon Door

Feature	Description
Station Type	Displays ACM Verify as the type of station used on the connected devices. A device that uses this station type of station is called an ACM Verify Station.
Managed or UnManaged	<p>Select if you want the ACM Verify Station managed or not.</p> <ul style="list-style-type: none"> • A managed 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. • An unmanaged ACM Verify 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.
Into Area	Select the Area where the ACM Verify Station is used to monitor access. Select the Don't Care option if the ACM Verify Station 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	<p>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 the ACM system.</p> <p>Tip: If the authentication type is Paired, the Door Add page re-displays with the Add Paired Device button.</p>

Options For VertX® and Mercury Security Doors

Feature	Description
Access Type	<p>Select the Access Type from the drop down list.</p> <p>Tip: If the access type is a paired door (paired master or paired slave), the Door Add page re-displays with the additional field, Paired Door. Select the Paired Door option from the drop down list.</p>
Door Mode	<p>The entry mode for the door when the door controller is online and communicating with the panel.</p> <p>For more information, see <i>Door Modes</i> on page 108</p>

Feature	Description
Offline Mode	<p>The entry mode used for the door if the door controller is no longer communicating with the panel.</p> <p>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.</p> <p>Select the Offline Mode option from the drop down list.</p>
Custom Mode	Select any additional door mode the door must support outside the Door Mode and Offline Mode options.
Custom Schedule	<p>Define when the Custom Mode would be active.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Masked Forced Schedule	<p>Define when Door Forced Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Masked Held Schedule	<p>Define when Door Held Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Always Mask Forced	<p>Check this box to specify that Door Forced Open alarms at this door are always masked.</p> <p>Normally, this box is unchecked.</p>
Always Mask Held	<p>Check this box to specify that Door Held Open alarms at this door are always masked.</p> <p>Normally, this box is unchecked.</p>

Door Processing Attributes for VertX® Doors

Feature	Description
Door use Tracking	<p>Select one of the listed options to define the level of door event tracking that is logged in the Monitor screen.</p> <ul style="list-style-type: none"> • None: only standard door events are logged • Used: includes the details of when the door is used • Used with pending: includes the events that occur between door use. <p>These options should only be used when the Detailed events option is enabled.</p>
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 display the current position of the door position switch (DPOS) in the Door

Feature	Description
	<p>State column of the Door Listing page. 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</p> <p>This feature is useful for circumstances where it is important to know all the details of an event.</p>
Enable Cipher Mode	<p>Check this box to enable cipher mode.</p> <p>Cipher mode allows the operator to enter card number digits at the door’s keypad.</p>
Do Not Log Rex Transactions	<p>Check this box to disable logging of request-to-exit transactions.</p>

Door Processing Attributes for Mercury Security Doors

Feature	Description
Log Grants Right Away	<p>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.</p> <p>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.</p>
Deny Duress	<p>Check this box to deny access to a user that indicates duress at a door.</p>
Don't Pulse Door Strike on REX	<p>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.</p> <p>If this box is not checked, the output is pulsed.</p> <p>For SimonsVoss wireless lock doors that do not support a door position switch (DPOS) , this box must not be checked.</p>
Require Two Card Control	<p>Check this box to specify that two tokens are required to open this door. This enforces two-person rule at a specified door.</p>
Door Forced Filter	<p>Check this box to enable the filter feature for door forced alarms.</p> <p>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.</p>
Log All Access as Used	<p>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.</p>
Detailed Events	<p>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.</p> <p>NOTE: To properly report the Door State from the Door Position Switch, Detailed Events must be enabled.</p> <p>Typically, five to ten detailed transactions will be generated for each grant transactions.</p>



Feature	Description
	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. 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.

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	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	<p>Specify the panel the door is assigned to.</p> <p>After you make your selection, new options may be displayed to define how the door is connected to the panel.</p>
Subpanel	<p>Specify the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the specified panel.</p>
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	<p>Select the Access Type for the door.</p> <p>Tip: If the access type is a paired door (paired master or paired slave), the Door Add page re-displays with the additional field, Paired Door. Select the Paired Door option from the drop down list.</p>

Feature	Description
Door Mode	Select the entry mode for the door when the door controller is online and communicating with the panel.
Offline Door Mode	<p>Select the entry mode used for the door if the door controller is no longer communicating with the panel.</p> <p>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.</p>
Custom Mode	Select any additional door mode the door must support outside the Door Mode and Offline Mode options.
Custom Schedule	<p>Define when the Custom Mode would be active.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Mask Forced Schedule	<p>Define when Door Forced Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Mask Held Schedule	<p>Define when Door Held Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
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	<p>Select one of the listed options to define the level of door event tracking that is logged in the Monitor screen.</p> <ul style="list-style-type: none"> • None: only standard door events are logged • Used: includes the details of when the door is used • Used with pending: includes the events that occur between door use. <p>These options should only be used when the Detailed events option is enabled.</p>
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	<p>Check this box to generate detailed events of all hardware at the door including door position masking, timer expiration and output status.</p> <p>This feature is useful for circumstances where it is important to know all the details of an event.</p>
Enable Cipher	Check this box to enable cipher mode.

Feature	Description
Mode	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 that are not supported by the door module may not be displayed.

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	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	<p>Specifies the panel the door is assigned to.</p> <p>After you make your selection, new options may be displayed to define how the door is connected to the panel.</p>
Subpanel	<p>Specifies the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the selected main panel.</p>
Door Number	<p>Specifies a configured group of readers, inputs, and outputs that are connected from the subpanel to the door.</p> <p>For wired connections, select the door number from the drop-down list.</p> <p>For wireless locks only:</p> <ul style="list-style-type: none"> Enter the number programmed for the lock. For all locks except SimonsVoss, select the number from the drop-down list.

Feature	Description
	<ul style="list-style-type: none"> For SimonsVoss wireless locks, enter the hexadecimal address assigned by the SmartIntego Tool. For more information, see <i>Configuring SimonsVoss Wireless Locks</i> on page 119.
Access Type	<p>Select the Access Type from the drop down list.</p> <p>Tip: If the access type is a paired door (paired master or paired slave), the Door Add page re-displays with the additional field, Paired Door. Select the Paired Door option from the drop down list.</p>
Door mode	<p>The entry mode for the door when the door controller is online and communicating with the panel.</p> <p>Select a Door Mode option from the drop down list.</p>
Offline Door Mode	<p>The entry mode used for the door if the door controller is no longer communicating with the panel.</p> <p>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.</p> <p>Select the Offline Mode option from the drop down list.</p>
Lock Function	<p>Select how the interior lock button will function.</p> <ul style="list-style-type: none"> 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. 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. 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. 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. <p>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).</p>
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.

Feature	Description
	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Mask Forced Schedule	<p>Define when Door Forced Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Mask Held Schedule	<p>Define when Door Held Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Always Mask Forced	<p>Check this box to specify that Door Forced Open alarms at this door are always masked.</p> <p>Normally, this box is unchecked.</p>
Always Mask Held	<p>Check this box to specify that Door Held Open alarms at this door are always masked.</p> <p>Normally, this box is unchecked.</p>
Door Processing Attributes	
Log grants right away	<p>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.</p> <p>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.</p>
Deny duress	Check this box to deny access to a user that indicates duress at a door.
Don't pulse door strike on REX	<p>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.</p> <p>If this box is not checked, the output is pulsed.</p> <p>For SimonsVoss wireless lock doors that do not support a door position switch (DPOS) , this box must not be checked.</p>
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	<p>Check this box to enable the filter feature for door forced alarms.</p> <p>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.</p>
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	<p>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.</p> <p>NOTE: To properly report the Door State from the Door Position Switch, Detailed Events</p>

Feature	Description
	must be enabled. 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. 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 - Edit Screen

When you click the name of an existing door from the Doors Listing page, the Doors 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®)* below
- *Door: Edit page (Mercury Security)* on page 149

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®)

When you click the **Parameters** tab on the Door Edit screen, the HID 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.
Installed	Check this box to indicate the appliance can communicate with the connected device.
Partitions	NOTE: If no partitions are defined for this system, this feature is not available. Select one or more partitions.

Feature	Description
	<p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	<p>Specify the panel the door is assigned to.</p> <p>After you make your selection, new options may be displayed to define how the door is connected to the panel.</p>
Subpanel	<p>Specify the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the specified panel.</p>
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	<p>Select the Access Type for the door.</p> <p>Tip: If the access type is a paired door (paired master or paired slave), the Door Add page re-displays with the additional field, Paired Door. Select the Paired Door option from the drop down list.</p>
Door Mode	Select the entry mode for the door when the door controller is online and communicating with the panel.
Offline Door Mode	<p>Select the entry mode used for the door if the door controller is no longer communicating with the panel.</p> <p>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.</p>
Custom Mode	Select any additional door mode the door must support outside the Door Mode and Offline Mode options.
Custom Schedule	<p>Define when the Custom Mode would be active.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Mask Forced Schedule	<p>Define when Door Forced Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Mask Held Schedule	<p>Define when Door Held Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
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.



Feature	Description
Door Processing Attributes	
Door use Tracking	<p>Select one of the listed options to define the level of door event tracking that is logged in the Monitor screen.</p> <ul style="list-style-type: none"> • None: only standard door events are logged • Used: includes the details of when the door is used • Used with pending: includes the events that occur between door use. <p>These options should only be used when the Detailed events option is enabled.</p>
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	<p>Check this box to generate detailed events of all hardware at the door including door position masking, timer expiration and output status.</p> <p>This feature is useful for circumstances where it is important to know all the details of an event.</p>
Enable Cipher Mode	<p>Check this box to enable cipher mode.</p> <p>Cipher mode allows the operator to enter card number digits at the door's keypad.</p>
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 New 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.
	<p>Click this button to delete this door.</p> <p>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 Listing page.</p>

Operations tab (VertX®)

When you click the **Operations** tab on the Door Edit screen, the Door Operations page is displayed. This page allows you to edit how the door operates, including the door mode, anti-passback and strike modes.



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	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	Specifies the panel the door is assigned to.
Subpanel	<p>Specifies the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the selected main panel.</p>
Lock Number	<p>The number ID for the set of inputs/outputs that are connected from the subpanel to the door.</p> <p>This option is only displayed if there are inputs or outputs connected to the selected subpanel.</p>
APB Mode	<p>Select the anti-passback mode for the door.</p> <p>For a description of each option, see <i>Anti-Passback Modes</i> on page 109.</p>
APB Delay	<p>Specifies the number of seconds before another entry is allowed.</p> <p>Enter the number of seconds.</p>
Into Area	<p>Identifies the area the user enters when passing through the door. If no area is specified, any location is valid.</p> <p>Select the area from the drop down list. Only those areas currently defined for this system appear in this list.</p>
Out of area	<p>Identifies the area the user moves into when exiting the door.</p> <p>Select the area from the drop down list.</p>
Strike Mode	<p>Defines 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.</p> <p>Select the strike mode from the drop down list.</p> <ul style="list-style-type: none"> • Cut short when open — the strike is deactivated on open • Turn off on close — the strike is deactivated on close. • Full strike time — the strike is deactivated when the timer expires.






Feature	Description
Held Pre-Alarm	<p>Specifies the number of seconds before the held open alarm is generated. Once the number of seconds is reached, a transaction will be generated which can be used to activate a warning signal.</p> <p>Enter the number of seconds.</p>
Minimum Strike Time	<p>Specifies 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.</p> <p>Enter the number of seconds. Default setting is 0 seconds.</p>
Standard Access time	<p>Specifies the standard number of seconds the strike will be activated.</p> <p>Enter the number of seconds. If the door is not opened within this interval, the door is automatically locked.</p>
Held Open time	<p>Specifies the number of seconds before the held open door event is generated.</p> <p>Enter the number of seconds.</p>
Extended Access	<p>Specifies the strike time for a door configured for persons that require more time to enter through a door.</p> <p>Enter the number of seconds.</p>
Extended Held Open Time	<p>Specifies the amount of time before the held open door event is generated for tokens marked with extended access.</p> <p>Enter the number of seconds.</p>
Card Formats	<p>Specifies the card formats that are compatible with the reader at the door.</p> <p>Check the box beside the card formats that apply.</p>
Simple Macros	
Type	<p>Select from the drop down list a default macro that is triggered when the following conditions are met for this door. Currently available macros include:</p> <ul style="list-style-type: none"> • Forced • Held • Pre-Alarm
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Output	From the drop down list, select an output that is activated by the Type condition.
Commands	<p>Click Save Macro to save the settings for this canned macro. If this is a new macro, a new row is automatically added below.</p> <p>Click Remove Macro to delete a macro. This button only appears if the macro has been saved in the system.</p> <p>For more information, see <i>Adding Simple Macros</i> on page 106.</p>

Feature	Description
	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.


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.
Installed	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	Specifies the panel the door is assigned to.
Subpanel	<p>Specifies the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the selected main panel.</p>
Lock Number	<p>The number ID for the set of inputs/outputs that are connected from the subpanel to the door.</p> <p>This option is only displayed if there are inputs or outputs connected to the selected subpanel.</p>
	To edit one of the readers, inputs or outputs that are connected to the door, click  beside the hardware item:


Feature	Description
	<ul style="list-style-type: none"> • If you click  beside the Reader or Alternate Reader, the Reader Edit page is displayed. • If you click  beside the Door Position, REX #1 or Rex#2, the Input Edit page is displayed. • 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.
Keypad decode	<p>From the drop down option list, select the keypad decode/encryption method you want to use for this reader. Choose from these options:</p> <ul style="list-style-type: none">• Hughes ID 4-bit• Indala• 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	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
	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	Check this box to indicate the appliance can communicate with the connected device.
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.
Debounce¹	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. Only the cameras that have been added to the system are listed.
Partitions	NOTE: If no partitions are defined for this system, this feature is not available. Select one or more partitions. Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item. Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.
	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.

¹Due 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 (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	Check this box to indicate the appliance can communicate with the connected device.
Address	The read-only address for this output point.
Partitions	NOTE: If no partitions are defined for this system, this feature is not available.
	Select one or more partitions.
	Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item. Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.
	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	Check this box to indicate the appliance can communicate with the connected device.
Partitions	NOTE: If no partitions are defined for this system, this feature is not available.
	Select one or more partitions.
	Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.

Feature	Description
	Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.
Panel	Specifies the panel the door is assigned to. 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. This option is only displayed if there is a subpanel connected to the selected main panel.
Lock Number	Enter the number ID for the set of inputs/outputs that are connected from the subpanel to the door. 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. The Available window is populated with those cameras that fit this definition. Click the Camera button beside this field to view live video from the camera. For more information on the video viewer window, see <i>Live Video Window</i> on page 165.
Available	This window displays a list of cameras that have been configured in the system. 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. 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. 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.
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.
Transaction Report	Click this button to generate a PDF transaction report on this door.

Feature	Description
Show Policy	Click this link to view a PDF report indicating the current policy associated with this door.

Events tab (VertX® doors)








When you click the **Events** tab from the Door: Edit screen, the list of events for the door is displayed.

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.

Feature	Description
---------	-------------

Local Events

This table is only displayed if there are local events for the device.

Name	The name of this event. Click the name to edit the local event.
Event	The event type.
Source Type	The source of this event.
Has On/Off	Indicates if this event possesses a toggle or on/off characteristic. Yes or No.
Masked	Indicates if this event is masked. Yes () or No (). Click the icon to change the status.
Logged	Indicates if this event is logged. Yes () or No (). Click the icon to change the status.
Show Video	Indicates if there is video associated with this event. Yes () or No (). Click the icon to change the status.
	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	Indicates if this event possesses a toggle or on/off characteristic. Yes or No.
Masked	Indicates if this event is masked. Yes or No.
Logged	Indicates if this event is logged. Yes or No.
Show Video	Indicates if there is video associated with this event. 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	Specify the event type. 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	Specify the priority of this event. The priority range is 1 - 999. The Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top.
Alarm Sound	Select an alarm sound that is played when a new alarm occurs while you are monitoring the Alarms page.
Suppress Time	Select a schedule when alarm events are not reported. Only schedules that have been defined in the system are listed.
Instructions	Enter any instructions that may be required for handling this event. The instructions are made available to the user on the Monitor screen.
Return Event	Select the event type of the RTN event.
Return Priority	Specify the priority of the RTN event. The priority range is 1 - 999.
Has on/off	Indicates that this event has an RTN event associated with it. NOTE: Adding return event information manually on this screen does not change the setting of this check box. It is set only if the original event has an associated RTN event defined for it.
Masked	Check this box to indicate that this a masked event by default. This can be changed on the Event List page.
Logged	Check this box to log the event by default. This can be changed on the Event List page.

Feature	Description
	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	<p>Check this box to auto-launch video from the linked camera feed when the event occurs by default. This can be changed on the Event List page.</p> <p>This feature only works if video is enabled.</p>
Two Person Required To Clear	<p>Check this box to specify that two people are required to acknowledge and clear this event.</p> <p>If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge.</p> <p>If the same operator attempts to clear the alarm, then nothing will happen.</p>
Email	<p>Enter the email address of all the people who should be notified when this event occurs.</p> <p>You can enter more than one email address separated by a comma.</p>
Roles:	
Available	<p>A list of all the roles that are available to you in the system.</p> <p>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.</p> <p>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.</p>
Members	<p>A list of all the roles that are able to view or edit this event.</p> <p>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.</p>
	Click this button to save your changes.
	Click this button to discard your changes.

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	<p>Lists the roles this access group is a member of.</p> <p>Click the + or - symbol beside each role to show or hide the identities that are in the access group through the role.</p>
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 that are not supported by the door module may not be displayed.

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	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	<p>Specifies the panel the door is assigned to.</p> <p>After you make your selection, new options may be displayed to define how the door is connected to the panel.</p>

Feature	Description
Subpanel	<p>Specifies the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the selected main panel.</p>
Lock Number or Door Number	<p>Specifies a configured group of readers, inputs, and outputs that are connected from the subpanel to the door.</p> <p>For wired connections, select the door number from the drop-down list.</p> <p>For wireless locks only:</p> <ul style="list-style-type: none"> Enter the number programmed for the lock. For all locks except SimonsVoss, select the number from the drop-down list. For SimonsVoss wireless locks, enter the hexadecimal address assigned by the SmartIntego Tool. For more information, see <i>Configuring SimonsVoss Wireless Locks</i> on page 119.
Access Type	<p>Select the Access Type from the drop down list.</p> <p>Tip: If the access type is a paired door (paired master or paired slave), the Door Add page re-displays with the additional field, Paired Door. Select the Paired Door option from the drop down list.</p>
Door Mode	<p>The entry mode for the door when the door controller is online and communicating with the panel.</p> <p>Select a Door Mode option from the drop down list.</p>
Offline Mode	<p>The entry mode used for the door if the door controller is no longer communicating with the panel.</p> <p>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.</p> <p>Select the Offline Mode option from the drop down list.</p>
Lock Function	<p>Select how the interior lock button will function.</p> <ul style="list-style-type: none"> 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. 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. 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. 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

Feature	Description
	<p>exterior may also be used to change status. Not to be used on mortise deadbolt.</p> <p>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).</p>
Custom Mode	Select any additional door mode the door must support outside the Door Mode and Offline Mode options.
Custom Schedule	<p>Define when the Custom Mode would be active.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Mask Forced Schedule	<p>Define when Door Forced Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Mask Held Schedule	<p>Define when Door Held Open alarms from this door will be masked.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Always Mask Forced	<p>Check this box to specify that Door Forced Open alarms at this door are always masked.</p> <p>Normally, this box is unchecked.</p>
Always Mask Held	<p>Check this box to specify that Door Held Open alarms at this door are always masked.</p> <p>Normally, this box is unchecked.</p>
Door Processing Attributes	
Log Grants Right Away	<p>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.</p> <p>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.</p>
Deny Duress	Check this box to deny access to a user that indicates duress at a door.
Don't Pulse Door Strike on REX	<p>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.</p> <p>If this box is not checked, the output is pulsed.</p>
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	<p>Check this box to enable the filter feature for door forced alarms.</p> <p>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.</p>

Feature	Description
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	<p>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.</p> <p>NOTE: To properly report the Door State from the Door Position Switch, Detailed Events must be enabled.</p> <p>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.</p>
Enable Cipher Mode	<p>Check this box to enable cipher mode.</p> <p>Cipher mode allows the operator to enter card number digits at the door's keypad.</p>
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 New 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.
	<p>Click this button to delete this door.</p> <p>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 Listing page.</p>

Operations tab (Mercury Security)

When you click the **Operations** tab on the Door Edit screen, the Operations page for the door is displayed. This page allows you to edit how the door operates, including the door mode, anti-passback and strike modes.

NOTE: Fields in this list that are not supported by the door module may not be displayed.

Feature	Description
Name	The name of the door.

Feature	Description
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	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	<p>Specifies the panel the door is assigned to.</p> <p>After you make your selection, new options may be displayed to define how the door is connected to the panel.</p>
Subpanel	<p>Specifies the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the selected main panel.</p>
Lock Number	<p>The number ID for the set of inputs/outputs that are connected from the subpanel to the door.</p> <p>This option is only displayed if there are inputs or outputs connected to the selected subpanel.</p>
Door Number	The number that has been assigned to the door module by the wireless lock configuration device.
APB Mode	<p>Select the Anti-Passback (APB) mode for the door.</p> <p>For more information on Anti-Passback modes, see <i>Anti-Passback Modes</i> on page 109.</p>
APB Delay	Enter the 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	<p>Select the area that the user enters by passing through the door.</p> <p>Only the areas that have been previously configured in the system appear in this list.</p>
Out of area	<p>Select the area that the user exits by passing through the door.</p> <p>Only the areas that have been previously configured in the system appear in this list.</p>
PIN Timeout	<p>Enter the number of seconds that a user is allowed to enter multiple PIN attempts before generating “Deny Count Exceeded” event.</p> <p>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.</p>
PIN	Enter the number of times a user can attempt to enter a PIN within the allotted PIN Timeout



Feature	Description
Attempts	time frame before an “Deny Count Exceeded” event is generated.
Strike Mode	<p>Select the strike mode.</p> <ul style="list-style-type: none"> • Cut short when open — the strike is deactivated when the door opens. • Full strike time — the strike is deactivated when the strike timer expires. • Turn off on close — the strike is deactivated when the door closes.
LED Mode	<p>Select the LED mode to specify how the reader LEDs are displayed.</p> <p>For more information on LED modes, see <i>LED Modes for Mercury Security</i> on page 183.</p>
Held Pre-Alarm	<p>Enter the number of seconds a door can be held open before a pre-alarm is issued.</p> <p>Instead of generating an alarm, it sends a warning signal to the Access Control Manager host.</p>
Access time when open	Enter the number of seconds the door remains unlocked after a card has been swiped.
Standard Access time	<p>Enter the number of seconds the door remains unlocked after access has been granted.</p> <p>If the door is not opened within this time, it will automatically lock.</p>
Held Open Time	Enter the number of seconds the door can be held open before a Door Held Open event is generated.
Extended Access	<p>Enter the number of seconds the door remains unlocked after access has been granted to token holders with extended access permissions.</p> <p>This feature is useful for users that may require more time to enter a door.</p>
Extended Held Open Time	<p>Enter the number of seconds the door can be held open for users with extended access permissions.</p> <p>This feature is useful for users that may require more time to enter a door.</p>
Card Formats	<p>Identify the card formats that the door accepts by moving them into the Members column if they are not already listed.</p> <p>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.</p> <p>When the door is created, the initial selection of card formats depends on:</p> <ul style="list-style-type: none"> • If there are 16 or less card formats defined in the system, all card formats are in the Members column. • If there are 17 or more card formats in the system, and: <ul style="list-style-type: none"> • 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. • 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. • If the door is created using a door template, and the template specifies: <ul style="list-style-type: none"> • No Change: The Members column is populated as described above.

Feature	Description
	<ul style="list-style-type: none"> Blank: Any selection from the panel is ignored and the Members column is empty. You must select the card formats accepted at the door. Assign: The contents of the Members column from the panel are replaced by the contents of the Members column from the door template. 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. 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	<p>Select a default macro that is triggered when the following conditions are met for this door. Currently available macros include:</p> <ul style="list-style-type: none"> Forced Held Pre-Alarm
Schedule	<p>Define when this macro can be triggered.</p> <p>Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.</p>
Op Type	Select an operation type used by this macro.
Output	Select an output that is activated by the 'Type' condition.
Commands	<p>Click Save Macro to save the settings for this canned macro. If this is a new macro, a new row is automatically added below.</p> <p>Click Remove Macro to delete a macro. This button only appears if the macro has been saved in the system.</p> <p>For more information, see <i>Adding Simple Macros</i> on page 106.</p>






The following options are always active:



Feature	Description
	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.
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 that are not supported by the door module may not be displayed.

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	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	<p>Specifies the panel the door is assigned to.</p> <p>After you make your selection, new options may be displayed to define how the door is connected to the panel.</p>
Subpanel	<p>Specifies the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the selected main panel.</p>
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.
	<p>To edit one of the readers, inputs or outputs that are connected to the door, click  beside the hardware item:</p> <ul style="list-style-type: none"> • If you click  beside the Reader or Alternate Reader, the Reader Edit page is displayed. • If you click  beside the Door Position, REX #1 or Rex#2, the Input Edit page is displayed. • If you click  beside Strike, the Output Edit page is displayed.



Feature	Description
Elevators	
The following options are only listed if the door is an elevator.	
Offline Access	<p>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.</p> <p>Select the elevator access level from the drop down list.</p> <p>Only the elevator levels that have been defined in the system are listed.</p>
Facility Access	<p>This identifies the elevator access level that this elevator defaults to if facility code mode is in effect.</p> <p>Select the elevator access level you require from the drop down list.</p> <p>Only the elevator levels that have been defined in the system are listed.</p>
Custom Access	<p>This identifies the elevator access level that this elevator defaults to when custom code mode is in effect.</p> <p>Select the elevator access level you require from the drop down list.</p> <p>Only the elevator levels that have been defined in the system are listed.</p>
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 New 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.

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	<p>Select the communication protocol used by the reader. The options include:</p> <ul style="list-style-type: none">• OSDP Avigilon recommends using OSDP 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.• F/2F.• D1/D0 (Wiegand)• CLK+Data (Mag) (NCI magnetic stripe standard)• Custom (Default) <p>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.</p>
The following options depend on the selected Reader Type and include:	
LED drive	<p>Select the LED drive mode for this reader. The options depend on the reader model and how it is wired and include:</p> <ul style="list-style-type: none">• None• Gen 1 wire• Reserved• Sep Red/Grn no buzz• Dorado 780• LCD• OSDP
Format by nibble	Check this box to indicate that this reader supports the format by nibble.
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.

Feature	Description
Inputs on reader	Check this box to indicate that this reader provides one or more input ports for serial input arrays.
Keypad decode	<p>Select the keypad decode/encryption method that is used by this reader. The options include:</p> <ul style="list-style-type: none"> • MR20 8-bit tamper • Hughes ID 4-bit • Indala • 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	<p>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.</p> <p>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.</p> <p>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.</p>
Baud Rate	<p>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.</p> <p>NOTE: Mercury controllers first try the setting provided and if that does not work, the controller will use default settings,</p>
OSDP Address	<p>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.</p> <p>NOTE: Mercury controllers first try the setting provided and if that does not work, the controller will use default settings,</p>
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	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view</p>

Feature	Description
	appear in this list. You can only see the partitions that you are a member of.
	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	Check this box to indicate the appliance can communicate with the connected device.
Address	The read-only address of this point.
EOL resistance	Select the End of Line resistance of this input. Only the EOL resistance that have been defined in the system are listed.
Debounce¹	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. 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. Only those cameras previously defined for this system appear in this window.
Partitions	NOTE: If no partitions are defined for this system, this feature is not available. Select one or more partitions. Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item. Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.
	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.

¹Due 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	Check this box to indicate the appliance can communicate with the connected device.
Address	The read-only address for this output point.
Operating Mode	Select how the panel knows when the output point is active. <ul style="list-style-type: none">• Energized When Active – a current is expected to pass through the output point when it is <i>active</i>.• Not Energized When Active – a current expected to pass through the output point when it is <i>inactive</i>.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
	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 tab is 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 that are not supported by the door module may not be displayed.

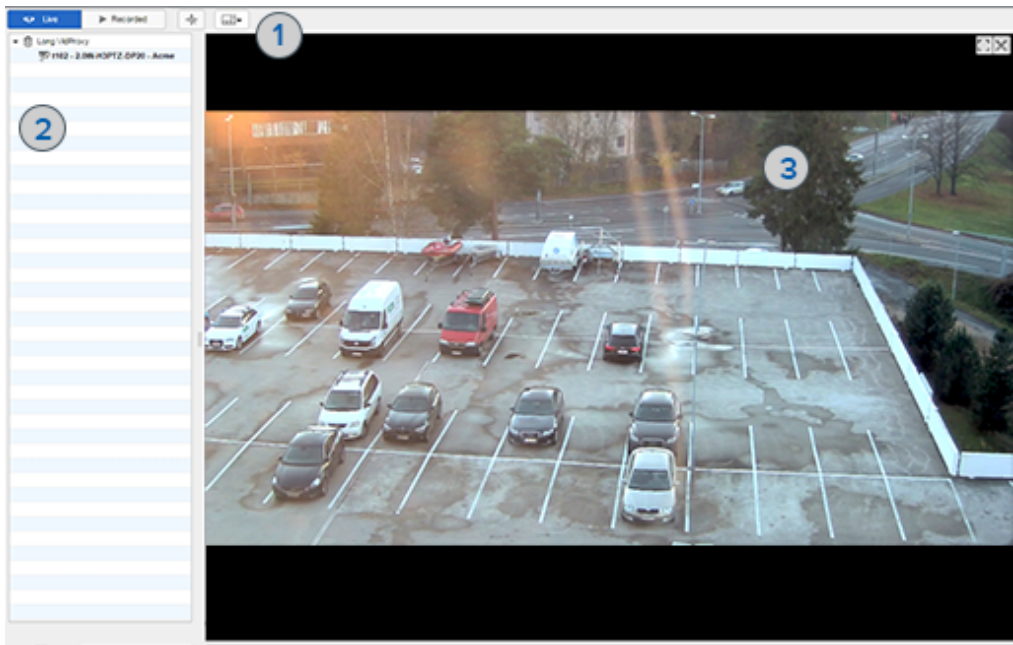
Feature	Description
Name	The name of the door.
Alt Name	The alternative name of the door.
Location	The location of the door.
Appliance	The appliance the door is connected to.
Vendor	The name of the door manufacturer.
Installed	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Panel	<p>Specifies the panel the door is assigned to.</p> <p>After you make your selection, new options may be displayed to define how the door is connected to the panel.</p>
Subpanel	<p>Specifies the subpanel that is connected to the door.</p> <p>This option is only displayed if there is a subpanel connected to the selected main panel.</p>
Lock Number	<p>Enter the number ID for the set of inputs/outputs that are connected from the subpanel to the door.</p> <p>This option is only displayed if there are inputs or outputs connected to the selected subpanel.</p>
Door Number	The number that has been assigned to the door module by the wireless lock configuration device.
Camera Type	<p>Select the external system that is connected to the camera.</p> <p>The Available window is populated with those cameras that fit this definition.</p> <p>Click the Camera button beside this field to view live video from the camera. For more information on the video viewer window, see <i>Live Video Window</i> on page 165.</p>
Available	<p>This window displays a list of cameras that have been configured in the system.</p> <p>To connect a camera to the door, select the camera from the Available list, then click  to move it to the Members list.</p>
Members	The window displays a list of cameras that are currently connected to the door.

Feature	Description
	To disconnect a camera from the door, select the camera from the Members list, then click  to move it to the Available list.
Search	<p>If you have more than 10 cameras, the Search feature may be displayed to help you find the cameras you need.</p> <p>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.</p>
	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.
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.

Live Video Window

When you click the **Camera** button from the Cameras page, the Live Video Window is displayed.

NOTE: The window may look different and have different controls depending on the external camera system that is connected to the Access Control Manager system.




Typically, the Live Video window will include the following elements:

	Feature	Description
1	Camera Controls Tool Bar	<p>This area includes all the features that you would need to view and control the related camera video.</p> <p>Options typically include switching from live to recorded video, PTZ controls for PTZ cameras, and changing the video display layout.</p>
2	Camera List	<p>This area lists all the cameras that are linked to the event.</p> <p>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.</p>
3	Image Panel	<p>This area displays the video stream from the connected cameras.</p> <p>In the top-right corner, you can minimize and maximize the display or close the video.</p>

Interlocks tab (Mercury Security)


When you click the **Interlocks** tab on the Door Edit screen, the Mercury Interlocks page is displayed. This page lists all the Interlocks that have been added to the system.

Feature	Description
Name	The name of the interlock. 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 Listing page, 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.
	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.
	Select the source type from the drop down list.
Source	Identifies the source of the interlock.
	Select the source from the drop down list. Options in this drop down list will vary depending on the source type specified.
Event Type	Identifies the event type the interlock is associated with.
	Select the Event Type from the drop down list. The options change to match the selected source option.
	Only those Event Types currently defined by the system appear in this list.
Event	Select the event that will trigger the interlock.
	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.
	Select an existing command from the drop down list.
	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.
	This option is not displayed if an argument is not required.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.

Interlock Edit page

When you click the name of an interlock from the Interlocks Listing page, the Interlock Edit page for the door is displayed.








Feature	Description
Name	Identifies the interlock. 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. Select the source type from the drop down list.
Source	Identifies the source of the interlock. Select the source from the drop down list. Options in this drop down list will vary depending on the source type specified.
Event Type	Identifies the event type the interlock is associated with. Select the Event Type from the drop down list. The options change to match the selected source option. Only those Event Types currently defined by the system appear in this list.
Event	Select the event that will trigger the interlock. 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. Select an existing command from the drop down list. 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. This option is not displayed if an argument is not required.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.

Events tab (Mercury Security doors)

When you click the **Events** tab from the Door: Edit screen, the list of events for the door is displayed.

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.

Feature	Description
Local Events	
This table is only displayed if there are local events for the device.	
Name	The name of this event. Click the name to edit the local event.
Event	The event type.
Source Type	The source of this event.
Has On/Off	Indicates if this event possesses a toggle or on/off characteristic. Yes or No.
Masked	Indicates if this event is masked. Yes () or No (). Click the icon to change the status.
Logged	Indicates if this event is logged. Yes () or No (). Click the icon to change the status.
Show Video	Indicates if there is video associated with this event. Yes () or No (). Click the icon to change the status.
	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	Indicates if this event possesses a toggle or on/off characteristic. Yes or No.
Masked	Indicates if this event is masked. Yes or No.
Logged	Indicates if this event is logged. Yes or No.
Show Video	Indicates if there is video associated with this event. 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.
Event Type	Specify the event type. 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	Specify the priority of this event. The priority range is 1 - 999. The Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top.
Alarm Sound	Select an alarm sound that is played when a new alarm occurs while you are monitoring the Alarms page.
Suppress Time	Select a schedule when alarm events are not reported. Only schedules that have been defined in the system are listed.
Instructions	Enter any instructions that may be required for handling this event. The instructions are made available to the user on the Monitor screen.
Return Event	Select the event type of the RTN event.
Return Priority	Specify the priority of the RTN event. The priority range is 1 - 999.
Has on/off	Indicates that this event has an RTN event associated with it. NOTE: Adding return event information manually on this screen does not change the setting of this check box. It is set only if the original event has an associated RTN event defined for it.
Masked	Check this box to indicate that this a masked event by default. This can be changed on the Event List page.

Feature	Description
Logged	<p>Check this box to log the event by default. This can be changed on the Event List page.</p> <p>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.</p>
Show Video	<p>Check this box to auto-launch video from the linked camera feed when the event occurs by default. This can be changed on the Event List page.</p> <p>This feature only works if video is enabled.</p>
Two Person Required To Clear	<p>Check this box to specify that two people are required to acknowledge and clear this event.</p> <p>If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge.</p> <p>If the same operator attempts to clear the alarm, then nothing will happen.</p>
Email	<p>Enter the email address of all the people who should be notified when this event occurs.</p> <p>You can enter more than one email address separated by a comma.</p>
Roles:	
Available	<p>A list of all the roles that are available to you in the system.</p> <p>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.</p> <p>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.</p>
Members	<p>A list of all the roles that are able to view or edit this event.</p> <p>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.</p>
	Click this button to save your changes.
	Click this button to discard your changes.

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	<p>Lists the roles this access group is a member of.</p> <p>Click the + or - symbol beside each role to show or hide the identities that are in the access group through the role.</p>
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](#)

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.

Feature	Description
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	Check this box to indicate the appliance can communicate with the connected device.
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	<p>Select if you want the ACM Verify Station managed or not.</p> <ul style="list-style-type: none"> • 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. • 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.
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	<p>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.</p> <p>Tip: If the authentication type is Paired, the Door Add page re-displays with the Add Paired Device button.</p>
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* below

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 174.
 - b. Enter the name to identify the device, such as "UserName'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 ACMclient 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 173.

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**.

Configuring Areas


Areas are zones that the Access Control Manager system assigns to define a physical area within a secured location. 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 cardholder 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.

For example, an anti-passback configuration can be used in a laboratory facility to restrict access to a specific room.

Adding Areas

1. Select **Physical Access > Areas**.

The Areas Listing page is displayed.

2. From the Areas Listing page, click **Add New Area**.
3. Enter a name for the area.
4. Select the appliance that will maintain the area details.
5. Select the **Enable Area** check box 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.

Areas - Editing

1. Select **Physical Access > Areas**.

The Areas Listing page is displayed.

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 .

Areas - Deleting

1. Select **Physical Access > Areas**.

The Areas Listing page is displayed.

2. From the Areas Listing page, 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 Access Control Manager 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 Listing page, 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**.
The HID Listing page is displayed.
2. From the HID Listing page, click **Add**.
The EOL Resistance Add page appears.
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 an VertX® input point:

1. Select **Physical Access > EOL Resistance > HID**.
The HID Listing page is displayed.
2. On the HID Listing page, 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 Listing page lists the available Mercury Security LED modes.

To make alterations to any of the available custom LED modes select that mode from the available listed options to open the mode on the *Mercury LED Mode Table <number> page*. For more detail, see *Editing Mercury Security 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 Mercury Security LED Modes







1. Select **Physical Access > Mercury LED Modes**.
2. Review the table details.
3. For any Door state, any of the following can be updated:
 - To change the color that display when the state becomes active, select the color by clicking inside the circle of the desired color (e.g.   ) in the On Color column.
 - To edit the time that the On color will display for, enter the new value in the On Time (1/10s) column. (The time is in 1/10th second ticks.)
 - To change the color to display when the door state is not active, select the color by clicking inside the circle of the desired color (e.g.   ) in the Off Color column.
 - To edit the repeat count (where this is possible), enter the new value in the Repeat Count column.
 - To edit the beep count (where this is possible), enter the new value in the Beep Count column.
4. Click  at the bottom of each page to save your changes.









Mercury Security LED Mode Table page

The **Mercury LED Mode Table <number>** page allows you to edit any of the available LED Mode tables.

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 on Mercury Security LED Modes, see *LED Modes for Mercury Security* on the next page.

Feature	Description
LED ID	Unique identifier for the LED state.
State	Door state that you can set a custom LED mode for.
On Color	Select the color to display when the door state is active.
	The options are green, amber, red or all off (  ). Click inside the circle of the desired color to select it (e.g.   ).

Feature	Description
On Time (1/10s)	Time in 1/10 th second ticks that the On color will display for.
Off Color	Select the color to display when the door state is not active. The options are green, amber, red or all off (  ). Click inside the circle of the desired color to select it (e.g.   ).
Off Time (1/10s)	Time in 1/10 th second ticks that the Off color will display for.
Repeat Count	Select the number of repeats for the on and off colors. NOTE: This will not be editable for some states.
Beep Count	Select the number of beeps to sound when the related state becomes active. 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 this to restore the selections for all states to the default setting.

LED Modes for Mercury Security

For Mercury Security door controllers, there are three reader LED modes.

The **Door mode** has function IDs 1 to 8. These are used when the reader is idle. Repeat and beep counts can not be set for these function IDs.

The **Door Processing Attributes** have function IDs 11 to 16. These are used when a card or pin is presented at the reader. Repeat count can be set for function 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.

Default Settings for LED Mode 1							
LED ID	On Color	Off Color	On Time	Off Time	Repeat Count	Beep Count	Door Mode or State of Door
1	Red	Off	29	1	0	0	Disable
2	Green	Off	29	1	0	0	Unlocked
3	Red	Off	29	1	0	0	Exit Only
4	Red	Off	1	29	0	0	Facility Code Only
5	Red	Off	1	29	0	0	Card Only
6	Green	Off	1	29	0	0	PIN Only
7	Red	Off	1	29	0	0	Card and PIN

LED ID	On Color	Off Color	On Time	Off Time	Repeat Count	Beep Count	Door Mode or State of Door
8	Green	Off	1	29	0	0	Card or PIN
11	Red	Off	2	2	5	3	Deny
12	Green	Off	2	2	7	1	Granted
13	Green	Off	1	14	0	2	User Command
14	Green	Red	1	4	6	2	Require two card control
15	Green	Red	4	1	25	2	Second User PIN
16	Green	Red	1	4	6	2	Wait

Default Settings for LED Mode 2

LED ID	On Color	Off Color	On Time	Off Time	Repeat Count	Beep Count	Door Mode or State of Door
1	Red	Off	29	1	0	0	Disable
2	Green	Off	29	1	0	0	Unlocked
3	Red	Off	29	1	0	0	Exit Only
4	Red	Off	24	1	0	0	Facility Code Only
5	Red	Off	24	1	0	0	Card Only
6	Red	Off	24	1	0	0	PIN Only
7	Red	Off	24	1	0	0	Card and PIN
8	Red	Off	24	1	0	0	Card or PIN
11	Red	Off	2	2	5	3	Deny
12	Green	Off	2	2	7	1	Granted
13	Green	Off	1	14	0	2	User Command
14	Green	Red	1	4	6	2	Require two card control
15	Green	Red	4	1	25	2	Second User PIN
16	Green	Red	1	4	6	2	Wait

Default Settings for LED Mode 3							
LED ID	On Color	Off Color	On Time	Off Time	Repeat Count	Beep Count	Door Mode or State of Door
1	Red	Off	29	1	0	0	Disable
2	Green	Off	29	1	0	0	Unlocked
3	Green	Off	29	1	0	0	Exit Only
4	Green	Off	29	1	0	0	Facility Code Only
5	Green	Off	29	1	0	0	Card Only
6	Green	Off	29	1	0	0	PIN Only
7	Green	Off	29	1	0	0	Card and PIN
8	Green	Off	29	1	0	0	Card or PIN
11	Red	Off	2	2	5	3	Deny
12	Green	Off	2	2	7	1	Granted
13	Green	Off	1	14	0	2	User Command
14	Green	Red	1	4	6	2	Require two card control
15	Green	Red	4	1	25	2	Second User PIN
16	Green	Red	1	4	6	2	Wait

For example, all three LED Modes have the same functionality for access grants, and the LED does not follow the strike time.

The Reader LED will flash to Green for seven repeat counts of 2.1 second ticks (2/10th seconds) on, 2.1 second ticks (2/10th seconds) off.

Configuring Card Formats


Readers that control access to doors come in many varieties and use many different card types. The ACM system supports the most commonly used card types using two 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.

This enables the qualified operator to define custom card formats, allowing a panel to control access for a variety of readers.


When you configure a door, you specify the card formats 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.

Adding Card Formats

1. Select **Physical Access > Card Formats**.
2. Click **Add New 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 Listing page, 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.

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 Access Control Manager 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 - Introduction* on page 246.

Searching for ACM System Events

The Access Control Manager 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. At the top of the Event Listing page, enter the name of the event in the **Name** field.

Tip: Use any series of letters and numbers to search for the events you want to see.

You can also use the drop down list options to specify that the name of the event **Starts With, Equals, Contains** or **Ends With** your search term.

2. If you know the event type that is assigned to the event, select one of the options in the **Event Type** drop down list.
3. Click **Search**.

The page refreshes to show your search results.

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**.

The Events list is displayed.

2. On the Events Listing page, 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.

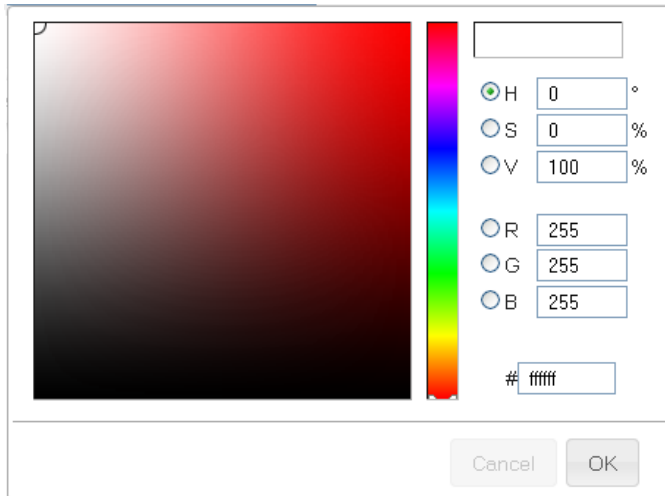
Assigning Priority Colors to ACM System Events

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 Listing page, 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:

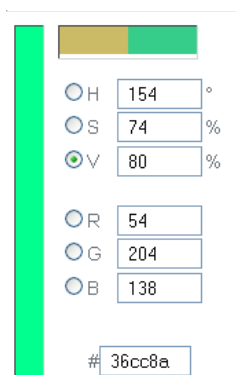
- a. From the HSV or RGB color fields, enter the general color you require.

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 three ways:

- Manually, from the Global Actions Listing page.
- By schedule, configured from the Global Actions Listing page.
- Automatically, when used in a Global Linkage.


One or more global actions must be defined before you can create Global Linkages.

Global Actions - Adding

1. Select **Physical Access > Global Actions**.
The Global Action Listing page is displayed.
2. On the Global Action Listing page, click **Add New Global Action**.
3. Enter the required details for this new global action.
4. Click  to save.

Once you've defined all the global actions that you need, proceed to the Global Linkages feature to create a chain of actions together.

Global Actions - Editing

1. Select **Physical Access > Global Actions**.
The Global Actions Listing page is displayed.
2. Click the name of the global action you need to modify.
3. Make the required changes.
4. Click  to save your changes.

Global Actions - Action Types


Feature	Description
Access Group Install/Uninstall	Specifies that one or more designated access groups are installed/uninstalled.
Action Group	Specifies action groups that are executed.
Door Install/Uninstall	Specifies that a designated door will be either installed or uninstalled.
Door Mode	Specifies the mode one or more designated doors will enter.
Door Grant	Specifies that entry is granted at one or more designated doors.
Door Mask	Specifies that alarms are forced to a masked/unmasked state at one or more

Feature	Description
	designated doors.
Email	Specifies email addresses and sends a predefined to those recipients.
Exacq Soft Trigger	Specifies a soft trigger that is executed on the Exacq camera system by the global action.
Input	Specifies that one or more designated inputs are masked/unmasked.
Intrusion Areas	Specifies all available commands for intrusion areas.
Intrusion Outputs	Specifies all available commands for intrusion outputs.
Intrusion Points	Specifies all available commands for intrusion points.
Output	Specifies that one or more designated outputs are activated/inactivated.
Panel Install/Uninstall	Specifies that one or more designated panels are installed/uninstalled.
Panel Macro	Specifies a macro routine to be run on a designated execute group.
Policy Install/Uninstall	Specifies that one or more designated policies are installed or uninstalled.
Schedule Set Mode	Specifies that one or more schedules are activated/inactivated/scanned.

Global Actions - Deleting

1. Select **Physical Access > Global Actions**.

The Global Actions Listing page is displayed.

2. From the Global Actions Listing page, 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**.

Global Actions - Intrusion Linkages and Actions

Noted below are some examples of setting-up intrusion linkages and actions.

Intrusion panel alarm due to an event in the ACM System

An ACM system event can trigger an intrusion alarm point. To set-up so that an alarm condition is generated at the intrusion panel (notifying the monitoring center etc.) due to an ACM system event (e.g. a forced door), ensure that the intrusion panel has a point with source "output" - 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 (e.g. silencing an alarm) can be made via intrusion panels.

Disable/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/access will be accessible from the keypad and from the **Monitor > 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 via a valid the ACM system card access can automatically disarm an area.

To allow a scenario where entry to an area via a valid card access disarms an intrusion area based on the cardholder's intrusion authorities, follow the steps below:

1. Create a global action to disarm an area. Action type of 'Intrusion Area', Subtype 'Master 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/disarmed from the keypad (depending on the tokens assigned to the identity) and from the **Monitor > Intrusion Status > Areas** section of the ACM system.



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.

Global Linkages - Adding

1. Select **Physical Access > Global Linkages**.
The Global Linkage Listing page is displayed.
2. On the Global Linkage Listing page, click **Add New Global Linkage**.
The Global Linkages Add page is displayed.
3. Enter the required details then click .
The screen refreshes to display the Global Linkage Edit page.
4. Edit each tab to add the required events, devices, identities and actions.
5. Click  to save your changes on each page.

Global Linkages - Editing

1. Select **Physical Access > Global Linkages**.
The Global Linkage Listing page is displayed.
2. On the Global Linkage Listing page, click the name of the global linkage that you want to edit.
The Global Linkages Edit page is displayed.
3. Edit each tab as required.
4. Click  after editing each page to save your changes.


Mustering - Introduction

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 Access Control Manager system.

1. Create an area for each muster station. For more information, see *Adding Areas* on page 180.
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 Listing page is displayed.
2. In the Map Templates Listing page, 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:

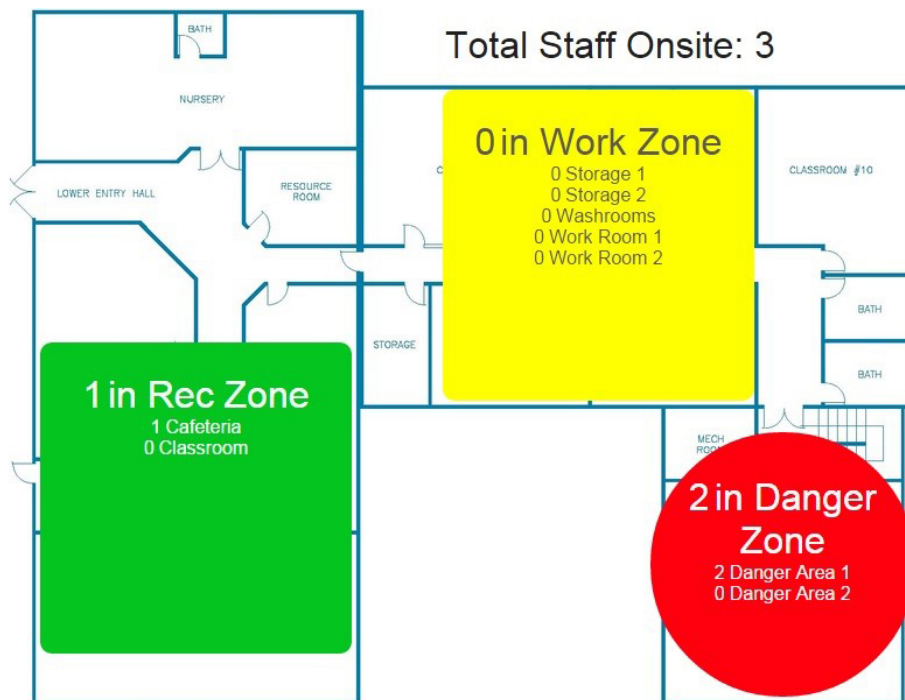
- a. In the **Area Group/Area** drop down list, select the muster area this dashboard element represents. You can select a specific area or a group of areas.
 - b. From the **Graphic Shape** drop down list, select Circle or Square.
 - c. Click the **Graphic Color** field to change the graphic shape color.
 - 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 279.

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 Listing page.



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.

Rec Zone

Show entries

Search:

First name ▲	Last name	Last badged location	Last badged time
John	Smith	Work Zone	11/12/2014 13:33:26

Showing 1 to 1 of 1 entries

[Previous](#) [Next](#)

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.


Mustering - Manually Moving Identities

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.
4. Click  .

Managing Appliances

When you log in to the Access Control Manager 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.

Appliances - Changes

Changes to appliances, including additions and deletions may be required after the original installation.

Adding Extra Appliances

NOTE: You can only add appliances if the system license supports multiple appliances.

Adding appliances increases the number of panels the system can support, and provides more storage for user data. Additional appliances are a requirement for replication and failover.

After you connect the new appliance to the network, complete the following steps to add the new appliance to the system:

1. In the top-right, select  > **Appliance**.

The Appliance Listing page is displayed.

2. Click the **Add Appliance** button.

The Appliance Add page is displayed.

3. Enter a new hostname for the appliance.


By default, the hostname for all appliances is the ACM system. You will need to set a new hostname for the appliance if an existing appliance already uses this hostname on the network.

4. Click  .

The new appliance automatically restarts. When you next log in to the system, you will see the new appliance in the Appliance Listing page.


Editing Appliances

After the appliance has been set up according to the *Getting Started Guide* included with the appliance, the Access Control Manager system is ready for use. You can now edit the system's default settings and set up the appliances backup and redundancy features.

1. In the top-right, select  > **Appliance**.

If there is only one appliance in this system, the Appliance Edit page is displayed.


If there is more than one appliance in this system, the Appliance Listing page is displayed. Select the appliance you want to edit.

2. Navigate through the tabbed pages to configure this appliance. The tabbed pages include:
 - **Appliance:** Use this page to edit the appliance properties, as well as shutdown or restart the appliance remotely.
 - **Access:** Use this page to specify and enable the controller panel types.
 - **Ports:** Use this page to specify how the appliance Ethernet ports are used to communicate with access control devices.
 - **Replication:** Use this page to set up system replication and redundancy.
 - **Backups:** Use this page to set up scheduled backups for this appliance.
 - **Logs:** Use this page to access the system logs.
 - **Software Updates:** Use this page to update the appliance software.
 - **About:** Use this page to see the current licenses, version numbers, and status of this appliance.
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 Listing page, 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

NOTE: Only the default Admin identity can edit the appliance Replication settings.

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.

Tip: It is recommended that replication be set up on all appliances before adding panels, other hardware or user details to the system. Once 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.

The replication feature allows two or more appliances to be set up to share a single set of [LDAP](#)¹ configuration data, where the appliances would be able to share identities and other system details. Any change made to configuration data on one appliance would automatically be copied (“replicated”) to the other appliances. This replication configuration 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 will be installed on one of the Peer appliances.

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.

¹Lightweight 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.

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

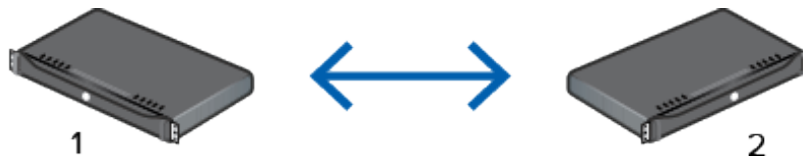
System Architecture for Replication

Replication works by automatically copying the [LDAP](#)¹ configuration databases from one appliance to 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.

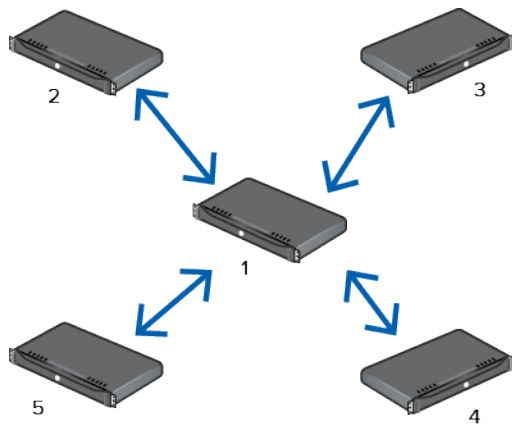
¹Lightweight Directory Access Protocol is an open, industry standard application protocol for accessing and maintaining distributed directory information services over a network. An LDAP database in the Access Control Manager system typically includes user details, connected hardware details, events, alarms and other system configuration details.



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.

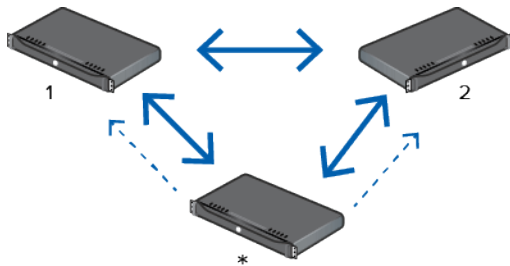
When configured and in standby mode, the Standby appliance is essentially a blank appliance that only has basic system settings. The Standby appliance has its own configuration for appliance related attributes such as host name, ports, time zone (etc.), but it does not have any hardware configuration 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.

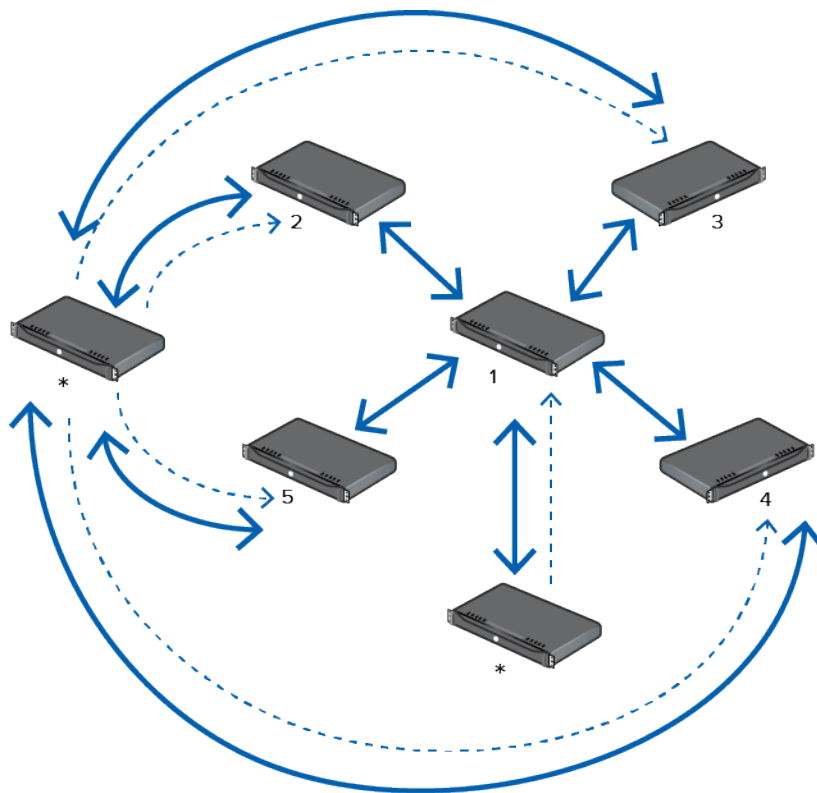
If one Primary appliance (1) exists for everyday operations and one Hot Standby appliance (*) is available, set up the Standby appliance to subscribe to and receive replicated configuration data and transactional data from the Primary appliance. If the Primary appliance fails, the Standby can automatically 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. Each appliance must either have a named server configured for this purpose, or a host file can be used for name resolution on each appliance if a DNS server is not available.
 - 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-master 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.
 - 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 203.

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** – give the appliance an appropriate name so that you can identify it on sight.
 - **Host Name** – the appliance's hostname on the network.
 - **Name Server** – the name or IP address of the DNS server used to resolve the appliance identity. If a DNS server is not available, then this can be left blank, and hosts file will need to be created on the appliance containing all the replicated appliance IP addresses and host names.
 - **Time Server** – enter 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** – enter the port number used for accessing the appliance web service.
 - **LDAP Connect Port** – enter the port number used 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.

Appliance: Edit

Appliance Access Ports Replication Backups Logs Software Update About

Appliance Name: Primary1

System Name: Primary1

Host Name: Primary1

Name Server: 192.168.5.1

Time Server: pool.ntp.org

Time Zone: America - New York

☐ Hot Standby

☒ Enable Remote TCP/IP Management

Splunk URL:

APB reset Reboot Appliance Shutdown Appliance

12/16/2015 11:01:57

Set Date/Time

Stored Transactions: 1000000

Hardware Type: Enterprise

Web Server Port: 443

Service Port: 6050

Edge Listen Port:

LDAP Connect Port: 5433

Transactions Connect Port:

Mercury Client Port:

☐ Mercury Require TLS

Tactical Settings:

Tactical Master:

☐ Manage Hardware

☐ Transfer Events

SMTP Server:

SMTP Port:

SMTP Host Name:

☐ Use Start TLS

☐ Use TLS

SMTP Mail From:

SMTP User:

SMTP Password:

Figure 5: Primary Appliance Tab

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** – give the appliance an appropriate name so that you can identify it on sight.
 - **Host Name** – the appliance's hostname on the network.
 - **Name Server** – the name or IP address of the DNS server used to resolve the appliance identity (use the same value as the replication address 1 appliance if possible), or blank if a hosts file will be created on the appliance containing all the replicated appliance IP addresses and host names.

- 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.

- If this is a Standby appliance, select the **Hot Standby** check box. Also, ensure that the 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 check box 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.

Appliance: Edit

Appliance	Access	Ports	Replication	Backups	Logs	Software Update	About
-----------	--------	-------	-------------	---------	------	-----------------	-------



Appliance Name:	<input type="text" value="Hot_Standby"/>	APB reset	Reboot Appliance	Shutdown Appliance
System Name:	<input type="text" value="Hot_Standby"/>	12/16/2015 11:05:16		
Host Name:	<input type="text" value="Hot_Standby"/>	Set Date/Time <input type="text"/>		
Name Server:	<input type="text" value="192.168.5.1"/>	Stored Transactions:	<input type="text" value="4000000"/>	
Time Server:	<input type="text" value="pool.ntp.org"/>	Hardware Type:	<input type="text" value="Enterprise"/>	
Time Zone:	<input type="text" value="America - New York"/>	Web Server Port:	<input type="text" value="443"/>	
<input checked="" type="checkbox"/> Hot Standby		Service Port:	<input type="text" value="6050"/>	
<input checked="" type="checkbox"/> Enable Remote TCP/IP Management		Edge Listen Port:	<input type="text"/>	
Splunk URL:	<input type="text"/>	LDAP Connect Port:	<input type="text" value="5433"/>	
		Transactions Connect Port:	<input type="text"/>	
		Mercury Client Port:	<input type="text"/>	
		<input type="checkbox"/> Mercury Require TLS		
Tactical Master: <input type="text"/>		SMTP Server:	<input type="text"/>	
<input type="checkbox"/> Manage Hardware		SMTP Port:	<input type="text"/>	
<input type="checkbox"/> Transfer Events		SMTP Host Name:	<input type="text"/>	
		<input type="checkbox"/> Use Start TLS		
		<input type="checkbox"/> Use TLS		
		SMTP Mail From:	<input type="text"/>	
		SMTP User:	<input type="text"/>	
		SMTP Password:	<input type="text"/>	

Figure 6: Hot Standby Appliance tab

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 check box.
 - b. **Enable Encryption** it is recommended that you select this check box 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.

Appliance: Edit

Appliance

Access

Ports

Replication

Backups

Logs

Software Update

About

Appliance: [Primary1](#)

Replication Settings

☒ Enable Replication

☒ Enable Encryption

Address: (Must be unique across enterprise)
(One system must have address '1')

Identity Password:

Event Replication Port:

Initial Retry Time: Seconds

Initial Retry Count:

Last Retry Time: Seconds

Last Retry Count: '0' for unlimited

Timeout: Seconds

Network Timeout: Seconds

Keep Alive: ###:##

Replication Subscriptions [New](#)No subscriptions exist. Press 'New' to create one. [Replication Update](#)

Status

RID	CSN	Name
0	12/16/2015 16:08:29.965626000 +00:00	Appliance record not in LDAP

No configuration entries.

Transaction replication status

No Transaction Replication Data.

Failover Settings

Standby Appliance:

☐ Monitor On

TCP Port:

☒ Active


Heartbeat Time: Seconds

Heartbeat Count:

Figure 7: 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 check box.
 - b. **Enable Encryption**: it is recommended that you select this check box 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.

Appliance: Edit

Appliance
Access
Ports
Replication
Backups
Logs
Software Update
About

Appliance: [Hot_Standby](#)

Replication Settings

☒ Enable Replication
☒ Enable Encryption
Address: (Must be unique across enterprise)
(One system must have address '1')
Identity Password:
Event Replication Port:

Initial Retry Time: Seconds
Initial Retry Count:
Last Retry Time: Seconds
Last Retry Count: '0' for unlimited
Timeout: Seconds
Network Timeout: Seconds
Keep Alive: ##:##:##

Replication Subscriptions New

No subscriptions exist. Press 'New' to create one. Replication Update

RID	CSN	Name
0	12/16/2015 16:11:49.430397000 +00:00	Appliance record not in LDAP

No configuration entries.

Transaction replication status

No Transaction Replication Data.

Failover Settings

Appliances
being
Monitored
Appliance Active

Figure 8: 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.

Appliance: [Hot Standby](#)

Replication Settings

☒ Enable Replication
 ☒ Enable Encryption

Address: (Must be unique across enterprise)
(One system must have address '1')

Identity Password:

Event Replication Port:

Initial Retry Time: Seconds

Initial Retry Count:

Last Retry Time: Seconds

Last Retry Count: '0' for unlimited

Timeout: Seconds

Network Timeout: Seconds

Keep Alive: ##:##:##

Replication Subscriptions [New](#)

Host	Web Port	Ldap Port	Login	Password
Primary1	443	5433	repladmin

[Replication Update](#)

Status

RID	CSN	Name
0	12/16/2015 16:11:49.430397000 +00:00	Appliance record not in LDAP

No configuration entries.

Transaction replication status

No Transaction Replication Data.

Failover Settings

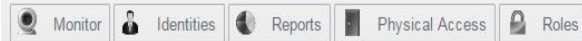
Appliances
being
Monitored
Appliance Active

Figure 9: 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.

Access Control Manager

avigilon access control



Replication Setup Process Log...

```
# Logfile created on 2015-12-16 11:26:41 -0500 by logger.rb/41954
I, [2015-12-16T11:26:41.065271 #4152] INFO -- : =====
I, [2015-12-16T11:26:41.065380 #4152] INFO -- : Starting Replication Setup Process. DATE: 20151216112641
I, [2015-12-16T11:26:41.065436 #4152] INFO -- : Saving my gateway info for gateway DN cn=e85cdd6cdfa442e1,ou=gateways,dc=plasec ...
I, [2015-12-16T11:26:41.393795 #4152] INFO -- : Saving my gateway replication subscriptions for gateway DN ou=replsubs,cn=e85cdd6cdfa442e1,ou=gateways,dc=plasec ...
I, [2015-12-16T11:26:41.404746 #4152] INFO -- : Backing up to compressed file /opt/PlaSec/rw/tmp/joinrepl
I, [2015-12-16T11:26:41.582723 #4152] INFO -- : Backing up binary db to compressed file /opt/PlaSec/rw/tmp/joinrepl-binary
I, [2015-12-16T11:26:41.638526 #4152] INFO -- : Determining cloud db...
I, [2015-12-16T11:26:41.650392 #4152] INFO -- : Extracting cloud db data from Primary1 5433 ...
I, [2015-12-16T11:26:41.968278 #4152] INFO -- : Extracting cloud binary db data from Primary1 5433 ...
I, [2015-12-16T11:26:41.986584 #4152] INFO -- : Stopping hal...
/opt/PlaSec/bin/monit: /opt/symas/lib/libcrypto.so.0.9.8: no version information available (required by /opt/PlaSec/bin/monit)
/opt/PlaSec/bin/monit: /opt/symas/lib/libssl.so.0.9.8: no version information available (required by /opt/PlaSec/bin/monit)
I, [2015-12-16T11:27:02.017153 #4152] INFO -- : hal is stopped.
I, [2015-12-16T11:27:02.017251 #4152] INFO -- : Stopping the database engine...
/opt/PlaSec/bin/monit: /opt/symas/lib/libcrypto.so.0.9.8: no version information available (required by /opt/PlaSec/bin/monit)
/opt/PlaSec/bin/monit: /opt/symas/lib/libssl.so.0.9.8: no version information available (required by /opt/PlaSec/bin/monit)
I, [2015-12-16T11:27:07.041865 #4152] INFO -- : Database engine is stopped.
I, [2015-12-16T11:27:07.041955 #4152] INFO -- : Clearing local database...
I, [2015-12-16T11:27:07.189465 #4152] INFO -- : Loading cloud data...
I, [2015-12-16T11:27:07.696051 #4152] INFO -- : Loading cloud binary data...
I, [2015-12-16T11:27:07.765933 #4152] INFO -- : Loading gateway data...
I, [2015-12-16T11:27:23.253516 #4152] INFO -- : Restarting slapd...
/opt/PlaSec/bin/monit: /opt/symas/lib/libcrypto.so.0.9.8: no version information available (required by /opt/PlaSec/bin/monit)
/opt/PlaSec/bin/monit: /opt/symas/lib/libssl.so.0.9.8: no version information available (required by /opt/PlaSec/bin/monit)
I, [2015-12-16T11:27:33.262898 #4152] INFO -- : Restarting hal...
/opt/PlaSec/bin/monit: /opt/symas/lib/libcrypto.so.0.9.8: no version information available (required by /opt/PlaSec/bin/monit)
/opt/PlaSec/bin/monit: /opt/symas/lib/libssl.so.0.9.8: no version information available (required by /opt/PlaSec/bin/monit)
I, [2015-12-16T11:27:33.272849 #4152] INFO -- : Initial Setup Complete.
I, [2015-12-16T11:27:33.272956 #4152] INFO -- : CONTINUE...
```

Figure 10: 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** in the top-right Setup links area, the Appliance Listing page should be displayed and list all appliances.

Appliances



Appliance Name	Host Name	Log Count	Mercury Security	HID	ISONAS	Kaba	CoreStreet	Delete
Primary1	Primary1	38	No	No	No	No	No	
Hot_Standby	Hot_Standby	38	No	No	No	No	No	





Figure 11: Appliance List page

Appliance: Primary1

Replication Settings

<input checked="" type="checkbox"/> Enable Replication	Initial Retry Time: <input type="text" value="10"/> Seconds
<input checked="" type="checkbox"/> Enable Encryption	Initial Retry Count: <input type="text" value="5"/>
Address: <input type="text" value="1"/> (Must be unique across enterprise) (One system must have address '1')	Last Retry Time: <input type="text" value="20"/> Seconds
Identity Password: <input type="password" value="....."/>	Last Retry Count: <input type="text" value="0"/> '0' for unlimited
Event Replication Port: <input type="text" value="6052"/>	Timeout: <input type="text" value="15"/> Seconds
	Network Timeout: <input type="text" value="30"/> Seconds
	Keep Alive: <input type="text" value="60:3:60"/> ##:##:##

Replication Subscriptions New

Host	Web Port	Ldap Port	Login	Password
<input type="text" value="Hot_Standby"/>	<input type="text" value="443"/>	<input type="text" value="5433"/>	<input type="text" value="repladmin"/>	<input type="password" value="....."/>

[Replication Update](#)

Status

RID	CSN	Name
1	12/16/2015 16:46:40.477325000 +00:00	Primary1
2	12/16/2015 16:46:40.214664000 +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

No Transaction Replication Data.

Failover Settings

Standby Appliance: <input type="text" value=""/>	<input type="checkbox"/> Monitor On
TCP Port: <input type="text" value=""/>	<input checked="" type="checkbox"/> Active
Heartbeat Time: <input type="text" value="0"/> Seconds	
Heartbeat Count: <input type="text" value="0"/>	

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 198.
 - 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

<input checked="" type="checkbox"/> Enable Replication	Initial Retry Time: 10 Seconds
<input checked="" type="checkbox"/> Enable Encryption	Initial Retry Count: 5
Address: 1 (Must be unique across enterprise) (One system must have address '1')	Last Retry Time: 20 Seconds
Identity Password:	Last Retry Count: 0 '0' for unlimited
Event Replication Port: 6052	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	<input checked="" type="checkbox"/> Monitor On
TCP Port: 8888	<input checked="" type="checkbox"/> Active
Heartbeat Time: 30 Seconds	
Heartbeat Count: 2	

Figure 13: Primary Replication tab, with Hot Standby configured

Appliance: [Hot_Standby](#)

Replication Settings

<input checked="" type="checkbox"/> Enable Replication	Initial Retry Time: <input type="text" value="10"/> Seconds
<input checked="" type="checkbox"/> Enable Encryption	Initial Retry Count: <input type="text" value="5"/>
Address: <input type="text" value="p"/> (Must be unique across enterprise)	Last Retry Time: <input type="text" value="20"/> Seconds
(One system must have address '1')	Last Retry Count: <input type="text" value="0"/> '0' for unlimited
Identity Password: <input type="password" value="....."/>	Timeout: <input type="text" value="15"/> Seconds
Event Replication Port: <input type="text" value="6052"/>	Network Timeout: <input type="text" value="30"/> Seconds
	Keep Alive: <input type="text" value="60:3:60"/> ##:##:##

Replication Subscriptions [New](#)

Host	Web Port	Ldap Port	Login	Password
Primary1	443	5433	repladmin

[Replication Update](#)

Status

RID	CSN	Name
1	12/16/2015 16:58:01.938319000 +00:00	Primary1
2	12/16/2015 16:58:02.337113000 +00:00	Hot_Standby

System Entries

RID	Provider	Retry	Timeout	Network	Timeout	KeepAlive
001	ldap://Primary1:5433/	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
Primary1	136	2015-12-16 11:56:48 -0500	2015-12-16 11:58:01 -0500	Success - processed 2 events that don't require replication

Failover Settings

Appliances being
Monitored

Appliance Active

Primary1 NO [Take Over](#)

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.

Appliance: Hot_Standby

Replication Settings

<input checked="" type="checkbox"/> Enable Replication	Initial Retry Time: <input type="text" value="10"/> Seconds
<input checked="" type="checkbox"/> Enable Encryption	Initial Retry Count: <input type="text" value="5"/>
Address: <input type="text" value="2"/> (Must be unique across enterprise)	Last Retry Time: <input type="text" value="20"/> Seconds
(One system must have address '1')	Last Retry Count: <input type="text" value="0"/> '0' for unlimited
Identity Password: <input type="password" value="....."/>	Timeout: <input type="text" value="15"/> Seconds
Event Replication Port: <input type="text" value="6052"/>	Network Timeout: <input type="text" value="30"/> Seconds
	Keep Alive: <input type="text" value="60:3:60"/> ##:##:##

Replication Subscriptions New

Host	Web Port	Ldap Port	Login	Password
Primary1	443	5433	repladmin

[Replication Update](#)

Status

RID	CSN	Name
1	12/16/2015 17:01:33.963728000 +00:00	Primary1
2	12/16/2015 17:01:37.683745000 +00:00	Hot_Standby

System Entries

RID	Provider	Retry	Timeout	Network Timeout	KeepAlive
001	ldap://Primary1:5433/	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
Primary1	136	2015-12-16 11:56:48 -0500	2015-12-16 12:01:33 -0500	Events send thread is terminating

Failover Settings

Appliances being Monitored

Appliance Active

Primary1 YES [Fail Back](#)

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 Listing page 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  .

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 Listing page is displayed.

2. In the right most column of the Ethernet Ports list, click **Routes**.

The Routes Listing page is displayed.

3. From the Routes Listing page, click **Add New Route**.

The Route Add page is displayed.

4. Complete the fields as required to define the new Ethernet route.

5. Click  .

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 Listing page 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** check box.

5. Complete the remaining fields as required to define the serial connection.

6. Click  .

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  .

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 Listing page 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/Subpanels* on page 93

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* on the next page.

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 Listing page 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.

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:
 1. Click on the name of the plan to open the Appliance Backup: Edit page.
 2. Enter the new name for the backup event.
 3. Leave the other fields as they are.
 4. 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:
 1. Click  to add a new backup event.
 2. Enter all the details for the backup event, specifying the location of the backup file to be restored.
 3. 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

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 Listing page is displayed.

2. Click the log you want to view.

The Appliances Log page displays.

Software Updates

Software updates are available for download and installation.

Updating the Appliance Software

Avigilon Access Control Manager software updates are available for download from the Avigilon website: [avigilon.com](https://www.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.


The Software Update Listing page is displayed.

2. Upload the latest version of the Access Control Manager software to the appliance.


- a. Click **Add New Software Update**.

The Software Update: Add New page is displayed.

- b. In the Upload Software file area, click the Browse button then locate the latest software file that was downloaded from the Avigilon website.

- 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.

The Software Update Listing page is automatically displayed when the software file has successfully uploaded to the appliance.

3. On the Software Update Listing page, click  beside the software file that you want to install on the appliance.
4. When the confirmation message is displayed, click **OK**.

The update progress is displayed in *Applying License Upgrades* on the next page. When the update is complete, the appliance will automatically reboot. You will need to log in to the appliance again.


Viewing the ACM SSL Certificate

Each ACM appliance in your network is assigned a self-signed Secure Socket Layer (SSL) certificate. When the SSL protocol is enabled on the appliance, this certificate can be used to verify the identity of an ACM appliance and securely encrypt the data traffic between the ACM appliance and other servers in your network.

An SSL certificate contains a SHA-1 fingerprint and a SHA-256 fingerprint. For authentication purposes, the SHA-256 fingerprint is used to verify the validity of a certificate. Any time an ACM appliance enabled to use the SSL protocol connects to another SSL-enabled server, it presents its SSL certificate. The first time it is presented, an administrator of the other server must accept, or trust, that certificate. From then on, as long as the ACM appliance presents the certificate with the same SHA-256 fingerprint, it can automatically connect. However, if ever the fingerprints do not match, the connection is denied until the reason for the mismatch is understood.

Only ACM system administrators with the delegation "SSL Certificate List" assigned to their role can view the SSL Certificate of the ACM server.

To view the SSL certificate,:

1. In the top-right, select  > **Appliance**.
2. Select the **SSL Certificate** tab.

The SSL certificate is displayed.

Appliances - About


The About section for appliances provides access to:

- review the appliance status
- the end user license agreement, and
- license and license key details.


Applying License Upgrades

When you purchase the appliance, it arrives licensed to support the features that you have ordered. As you set up and use your system, you may find that you need additional features.

To upgrade the system license, complete the following:

1. Purchase a license upgrade from Avigilon. You will be given a new license and license key file.
2. Copy the license (.lic) and license key (.key) files to your desktop.
3. Log in to the Access Control Manager appliance.
4. In the top-right, select  > **Appliance**.
5. Select the **About** tab.

The About page is displayed.

6. In the License area, click the file navigation button then locate the license (.lic) file.
7. In the License Key area, click the file navigation button then locate the license key (.key) file.
8. Click .

If the license provides access to new features, you may be asked to accept a new End User License Agreement. For more information, see *Accepting the End User License Agreement* below.

Viewing the End User License Agreement

Follow the steps below to view the End User License Agreement:

1. Select **Appliance > About**.
2. Click **View End User License Agreement Terms and Conditions** on the Appliance: Edit page.
3. Review the license agreement on the Appliance: Edit (End User License Agreement) page.
4. Click **Back** to return to the Appliance: Edit page.

Accepting the End User License Agreement

Before you can use the Access Control Manager system, you must accept the End User License Agreement.

You may have noticed this error message that is displayed on each page:

END USER LICENSE NOT YET ACCEPTED, SYSTEM WILL NOT RUN PROPERLY! PLEASE ACCEPT EULA TO STAY IN COMPLIANCE!

1. To access the End User License Agreement, click the link under the error message or select **Appliance > About > View End User License Agreement Terms and Conditions**.
2. On the End User License Agreement page, review the license agreement.
3. After reviewing the license agreement, select the check box next to the message *I accept the terms of the License Agreement*.
4. Click **Submit**.

The error message is removed and you can begin to configure the Access Control Manager system.

Reviewing the Appliance Status

From the Appliance Edit page, select the **About** tab.

At the bottom of the About page are the appliance status details. Each item listed in the Appliance Diagnostic Information area is highlighted in a specific color to identify its status. For more information about the status colors, see *Status Colors* on page 37.

You can also review the appliance hardware status from the Monitor screen. For more information, see *Monitor - Dashboard* on page 31.

Managing Collaborations


Collaborations allow the Access Control Manager to exchange data with third party databases and applications. 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.

Collaborations - Adding

To add a collaboration:

1. Select  > **Collaboration**.
The Collaborations Listing page appears.
2. Click **Add New 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, if required.
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 to Export; Include Primary Photo; Include Roles; Location Type; Host; Port Number; User Name; Password; Location; Domain Name (Windows Share)
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
	NOTE: Ensure any individual images to be imported are not over 1MB.

6. Click .

The Collaboration: Edit screen appears.

7. Navigate through the tabbed pages and fill out the details as required.

8. Click .

Collaborations - Adding Events XML Collaboration

To add an Events XML collaboration:

1. Select  > **Collaboration**.

The Collaborations Listing page appears.

2. Click **Add New Collaboration**.

The Collaboration: Add New page appears.

3. Complete the following fields:

Field	Description
Name	Name for the collaboration.
Appliance	Select the appropriate Appliance, if more than one appliance is available.
Type	Select Events – Generic XML. NOTE: The following additional fields display once the type is selected: <ul style="list-style-type: none"> • Host • Require TCP • 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 .

The message 'Collaboration entry was successfully created' displays on the Collaboration: Edit screen.

5. Click the **Events** tab.
6. Complete the following fields:

Field	Description
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 .

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 236.

XML	Definition
<code><plasectrxGatewayDN> cn=544de4aa06914073,ou=gateways ,dc=plasec </plasectrxGatewayDN></code>	An internal reference for the ACM appliance that this XML came from.
<code><cn>38901f4a95d14013</cn></code>	The unique row identifier for this particular event. Corresponds to the ID column in the history tables.
<code><plasectrxRecdate>20140610055028-0700 </plasectrxRecdate></code>	Time the event was logged into the ACM system history – adjusted for ACM local time.
<code><plasectrxPanel date>20140610085028-400 </plasectrxPanel date></code>	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.
<code><plasectrxRecdateUTC>20140610125028Z </plasectrxRecdateUTC></code>	Time the event was logged into the ACM system history.
<code><plasectrxPanel dateUTC>20140610125028Z </plasectrxPanel dateUTC></code>	The UTC time the event actually happened. It is the timestamp of the event being reported up from the field hardware.
<code><plasectrxLastacc> 19700101000000Z</plasectrxLastacc></code>	Last Access time and date of the Token that is associated with this event. Example – the last

XML	Definition
	recorded valid access of the card that was used at a door causing a 'Local Grant' event.
<code><plasectrxEvttypename></code> Intrusion <code></plasectrxEvttypename></code>	ACM event type category for this event. Corresponds to one of the event types defined in the ACM system in Settings: Event Types.
<code><plasectrxBackgroundColor></code> <code></plasectrxBackgroundColor></code>	Color assigned to the event background color (if any) for display in the ACM monitor.
<code><plasectrxForegroundColor></code> <code></plasectrxForegroundColor></code>	Color assigned to the event foreground color (if any) for display in the ACM monitor.
<code><plasectrxAckBackgroundColor></code> <code></plasectrxAckBackgroundColor></code>	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.
<code><plasectrxAckForegroundColor></code> <code></plasectrxAckForegroundColor></code>	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.
<code><plasectrxEventname></code> Input point in alarm <code></plasectrxEventname></code>	Name of the event. Corresponds to one of the events defined in the ACM system in Physical Access: Events.
<code><plasectrxPanel name></code> elevator test <code></plasectrxPanel name></code>	Name of the panel that the event originated from.
<code><plasectrxSourcename></code> Input on subpanel 0 Address 1 <code></plasectrxSourcename></code>	Name of the source of the event.
<code><plasectrxSourcelocation></code> <code></plasectrxSourcelocation></code>	Location of the source of the event, as defined in the 'Location' field on the various hardware property pages.
<code><plasectrxSourcealtname></code> <code></plasectrxSourcealtname></code>	Applies to doors only - if the event source is a door, this is the Alt. Name as defined on the Door properties Configuration tab.
<code><plasectrxPointaddress></code> 750 <code></plasectrxPointaddress></code>	A reference number for the event e.g. 'Input point in alarm'.
<code><plasectrxPointDN></code> cn=750,ou=points,dc=plasec <code></plasectrxPointDN></code>	This is the LDAP dn of the 'Input point in alarm' event, for lookup during ACM processing.
<code><plasectrxEvttypeaddress></code> 5 <code></plasectrxEvttypeaddress></code>	This is a reference number for the event type e.g. 'Intrusion'.
<code><plasectrxSourceDN></code> cn=100,cn=0,cn=9,ou=panels, cn=544de4aa06914073,ou=gateways, dc=plasec <code></plasectrxSourceDN></code>	LDAP dn of the source of the event, used in ACM processing.

XML	Definition
<pre><plasectrxSourcetype>40 </plasectrxSourcetype></pre>	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.
<pre><plasectrxOperatorname> </plasectrxOperatorname></pre>	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.
<pre><plasectrxPri>10</plasectrxPri></pre>	Priority of the event, as defined on the Event properties page.
<pre><plasectrxMsg></plasectrxMsg></pre>	Contents of the 'Message' column in the Monitor e.g. the raw card data from an 'Invalid Card Format' event.
<pre><plasectrxIdentityDN> </plasectrxIdentityDN></pre>	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.
<pre><plasectrxCardno>0 </plasectrxCardno></pre>	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.
<pre><plasectrxEmbossedno> </plasectrxEmbossedno></pre>	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.
<pre><plasectrxLname> </plasectrxLname></pre>	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.
<pre><plasectrxFname> </plasectrxFname></pre>	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.
<pre><plasectrxMi></plasectrxMi></pre>	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.
<pre><plasectrxIssuelevel>-1 </plasectrxIssuelevel></pre>	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.
<pre><plasectrxFacilityCode>0 </plasectrxFacilityCode></pre>	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.
<pre><plasectrxExpiredat> 19700101000000Z </plasectrxExpiredat></pre>	Deactivate date of the token that is associated with this event. Example – the deactivate date of

XML	Definition
	the card that was used at a door causing a 'local grant' event.
<pre><plasectrxActivdat> 19700101000000Z </plasectrxActivdat></pre>	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.
<pre><plasectrxIssuedat> 19700101000000Z </plasectrxIssuedat></pre>	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.
<pre><plasectrxHasCamera>0 </plasectrxHasCamera></pre>	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.
<pre><plasectrxHasNotes>0 </plasectrxHasNotes></pre>	Indicates whether there are any notes available for this event.
<pre><plasectrxHasSoftTriggerSet>0 </plasectrxHasSoftTriggerSet></pre>	Indicates whether there is a soft trigger associated – currently this applies to Exacq video integration only.
<pre><plasectrxShowVideo>0 </plasectrxShowVideo></pre>	Indicates whether the event is optioned to show pop-up video of an associated camera.
<pre><plasectrxSeqno>0 </plasectrxSeqno></pre>	Not used.
<pre><plasectrxIsAlarm>1 </plasectrxIsAlarm></pre>	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</plasectrxGatewayDN>

  <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>
<plasectrxEvttypeaddress> 5</plasectrxEvttypeaddress>
<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>



<?xml version="1.0" encoding="ISO-8859-1"?>

```

For definitions of the individual attributes, refer to *Collaborations - Events XML Definitions* on page 233.

Collaboration - Editing

To edit an existing collaboration:

1. Select  > **Collaboration**.
The Collaborations Listing page 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  .

Collaboration - Types



The types of collaboration available in this application include:

Type	Description
Identity	
Identity CSV Export	Export identities, photos, tokens, groups, and roles using an updated CSV file.
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	Pull identities, tokens, groups, roles from a Microsoft SQL Server RDBMS store and

Type	Description
Server pull	keep the Access Control Manager identity database in sync with changes.
Events	
Events - Generic XML	Transmit events in real time using XML.
Events - Splunk	Produces messages in Splunk format. Splunk is a log aggregation product.



Collaboration - Running

To run a collaboration:

1. Select  > **Collaboration**.
The Collaboration Listing page appears.
2. Click  from the **Run** column next to the collaboration you want to run.
3. When the confirmation message is displayed, click **OK**.



Collaboration - Deleting


To delete an existing collaboration:

1. Select  > **Collaboration**.
The Collaboration Listing page appears.
2. Click  beside the collaboration that you want to delete.
3. When the confirmation message is displayed, click **OK**.

Collaboration - Assigning Events to a Collaboration

To assign an event type to a collaboration:


1. Select  > **Collaboration**.
2. From the Collaboration Listing page, 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  .

Setup & Settings

When you click or hover on , the following options are displayed:

- [Appliance](#) — This feature enables the operator to connect, customize and set up your appliance to meet your system requirements.
- [Collaboration](#) — This feature enables the operator to set-up and manage collaborations which exchange data with third party databases and applications.
- [Schedules](#) — This feature enables the operator to define periods of time that can be used to control such things as when a door is accessible, when a card is valid, or when a device is activated.
- [Holidays](#) — This feature enables the operator to define specific days during which normal rules are suspended for one or more schedules.
- [Event Types](#) — This feature enables the operator to define additional event types and provide instructions on how to handle an event generated in the Access Control Manager system.
- [User Fields](#) — This feature enables the administrator to create fields, in addition to the factory default fields, that are used for enrolling Identities.
- [User Lists](#) — This feature enables the operator to define additional options for those fields on the Identity page with drop down option lists.
- [System Settings](#) — This feature enables the operator to define basic values within the system, like system settings language, token expiration time, and required password strength.
- [Paired Devices](#) — This feature enables the operator to generate a one-time key to connect a browser-enabled device such as a smartphone to a door configured as an ACM Verify station so that it can function as a Virtual Station.
- [Badge Designer](#) — This feature enables the operator to create and customize a badge layout (a badge template) for use by badge holders.
- [External Systems](#) — This feature enables the operator to define and configure a camera or other image capture device for use by this application.
- [Maps](#) — This feature enables the qualified operator to create maps and populate them with input, output, and alarm points.

Schedules and Holidays - Introduction

Schedules

A schedule is a reusable time template that can be used to control when a system setting is active. A user's access privileges are the result of a three-way relationship that is created between: (1) a group of users, (2) a secured device and (3) a schedule.

For example, you can apply a schedule to a group of users and doors to limit their access permissions to the days and times specified in the schedule.

A door can also 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.

NOTE: When a panel appears to be functioning in an unexpected way, check the event log for the "Panel Schedule Count Exceeded" event. A panel can accommodate a maximum of 255 schedules. This event is recorded in the system log when the number of schedules configured for a panel exceeds the maximum. To correct this, fewer schedules need to be assigned to the panel. You can identify unneeded schedules on the Panels - Schedules tab, or you can move hardware to a different or new panel.

Holidays

Holidays are special days in the year when the standard schedule does not apply, or because 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 will need to update the system holidays each year.

Adding Schedules

1. Select  > **Schedules**.

The Schedules Listing page is displayed.

2. From the Schedules Listing page, click **Add New Schedule**.
3. On the Schedule Add New page, enter a name for the schedule.
4. Select the schedule mode:
 - **ON** – the schedule is constantly on. You do not need to set specific dates or times for the schedule.
 - **OFF** – the schedule is off.
 - **SCAN** – the schedule follows the date and time settings defined through the check boxes for each row of time.
5. Select all the days of the week (Sun-Sat) and holidays (1-8) this schedule applies to.
6. Enter the start (Active) and end (Inactive) time for the specified days for each row. The time must be in 24 hr format.

NOTE: Beware that the time entered includes the full minute. So, if 17:00 was entered as an Inactive time, the actual inactive time will be 17:00:59. Active times, on the other hand, commence on the time entered. So, if 09:00 is entered as the Active time, the actual active time will be 09:00:00.

7. If required, you can enter multiple rows of time and days to meet your requirements.

NOTE: Ensure that you consider related Inactive times when entering Active times for alternative schedules. For example, if you entered a Day Shift schedule for 08:00 to 20:00 and a Night Shift for 20:00 to 08:00, then conflicts will occur. The Night Shift schedule will not commence as scheduled as it will try to start at 20:00:00 but the Day Shift schedule will still be active until 20:00:59. Similarly, if the Night Shift Schedule was active then the Day Shift could not commence at 08:00:00.


To solve the above issue the Day Shift schedule would be set to 08:00 to 19:59 and the Night Shift would be set to 20:00 to 07:59.

8. Click  to save the new schedule.

Editing Schedules



1. Select  > **Schedules**.

The Schedules Listing page is displayed.

2. From the Schedules Listing page, click the name of the schedule you want to edit.
3. Edit the schedule as required.
4. Click  to save your changes.

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**.

Holidays - Adding

1. Select  > **Holidays**.

The Holidays Listing page is displayed.


2. From the Holidays Listing page, click **Add New Holiday**.
3. On the Holiday: Add New page, enter a name for the holiday.
4. Enter the specific date of the holiday.

NOTE: If this is a recurring holiday, you will need to create a holiday for each instance of this holiday or update the date each year.


5. If the holiday spans more than one day, enter the number of days the holiday spans for in the **Additional Days** field.


If the setting is **0**, the holiday only spans the one date entered in the previous step.

For example, you entered 01/01/2017 as the date of the holiday and entered 2 for the Additional Days field. This means the system expects the holiday to span for January 1, 2 and 3.


6. Enter the **Type** of holiday. (The holiday type number allows you to group specific types of holidays together.)
7. Define how you want the holiday schedule to be activated. The holiday must be assigned to a schedule to initiate any special actions.
 - Activate only the holiday schedule configured for the holiday dates — leave the **Preserve schedule days** check box *clear*. Only the schedule configured for the holiday will be active on the dates of the holiday.
 - Activate the holiday schedule configured for the holiday dates in addition to the regular schedule for that door — check the **Preserve schedule days** box. The schedule configured for the holiday and any other active schedule will be active on the holiday.
8. Click  to save the new holiday.


Holidays - Editing

1. Select  > **Holidays**.

The Holidays Listing page is displayed.
2. On the Holidays Listing page, 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.

Holidays - Deleting

1. Select  > **Holidays**.






The Holiday Listing page is displayed.
2. On the Holiday Listing page, click  for the holiday you want to delete.
3. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.

Holidays and Schedules - Examples

Noted below are two examples of setting up holidays/schedules.






Example 1: Part-Day Holiday

All staff are attending an afternoon team function on 18 December, with work finishing at noon. On the 18th we want the doors to unlock from 8am to 12pm, with access by card only mode after 12pm. The normal schedule for Monday to Friday is for the doors to open from 8am to 5pm. Steps to take are:

1. Select  > **Holidays**.
2. On the Holiday Listing page, click  to add a new holiday.
3. On the Holiday: Add New screen, enter the following then click  to save:
 - **Name** (e.g. Company Half Day).
 - **Date** (e.g. 12/18/2016).
 - **Type** (e.g. 8).
4. Select  > **Schedules**.
5. Select the normal schedule on the Schedules Listing page.
6. On the first available free line:
 - Click in the checkbox for the **Type** selected in step 3 above (e.g. 8), so that a checkmark displays.
 - On the same line enter 08:00 as the **Active** time, and 11:59 as the **Inactive** time.
7. Click  to save.

Example 2: Additional Access Time

A special delivery is scheduled for December 20, requiring additional access time from 8pm to 12am. In order to create the additional access time without impacting the normal daily schedule, the Preserve schedule days option can be used. This option allows you to set separate access schedules for the same day. Steps to take are:

1. Select  > **Holidays**.
2. On the Holiday Listing page, click  to add a new holiday.
3. On the Holiday: Add New screen, enter the following then click  to save:
 - **Name** (e.g. Late Night Access).
 - **Date** (e.g. 12/20/2016).
 - **Type** (e.g. 7).
 - Click in the **Preserve schedule days** checkbox.
4. Select  > **Schedules**.
5. Select the normal schedule on the Schedules Listing page.
6. On the first available free line:
 - Click in the checkbox for the **Type** selected in step 3 above (e.g. 7), so that a checkmark displays.
 - On the same line enter 20:00 as the **Active** time, and 23:59 as the **Inactive** time.
7. Click  to save.

Event Types - Introduction

Event types are classifications of events that may occur during the operation of the Access Control Manager 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 Panel 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: <ul style="list-style-type: none"> • Lock offline with hub • Panel offline • Radio disturbance • Subpanel communication disabled • Subpanel offline • Subpanel type mismatch • VidProxy Image Service offline • VidProxy Service offline
Door held open	Door	Covers door held events including: <ul style="list-style-type: none"> • Door held masked • Door held open • Door held open pre-alarm • Door held unmasked • Extended door held disabled • Extended door held enabled
Forced Door	Door	Covers forced door events including: <ul style="list-style-type: none"> • Forced door • Forced door masked • Forced door unmasked
Intrusion	Panel Subpanel Intrusion Panel Inputs	This event type is used in two circumstances – for Intrusion Panel events and for general purpose input events from Mercury Security or VertX® (general purpose inputs are inputs that are not used in a door). If the source type includes the word 'Intrusion' (e.g. Intrusion Point, Intrusion System, Intrusion Panel etc.) then it relates to intrusion panels. If the source type is Input, then it relates to an event generated by a general purpose (non-door) Mercury Security or VertX® input (e.g. Masked input point active, Input point in alarm, Input point masked).

Event Type	Source	Definition
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.).
Maintenance	Door Panel Subpanel	Primarily developed to cover events where action is required outside of the system (e.g. uploads, downloads, inconsistencies between panels etc.). 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: <ul style="list-style-type: none"> • Output point active • Output point inactive • 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. 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 Credentials	Covers events where a record has been added, deleted or updated by the system.
Tamper	Door Panel Subpanel	Relates to all tamper events for panels or doors, including (but not limited to): <ul style="list-style-type: none"> • Area disabled/enabled • Lock jammed • Occupancy count reached • Panel transaction level reached
User audit	Door Panel Subpanel Intrusion Panel System/ Database	Where a user makes a change in the UI or in REST, including (but not limited to): <ul style="list-style-type: none"> • APB requests • Door-related requests • Intrusion panel requests • Records changed in database
Valid Credential	Doors	Relates to any door event where access is granted (e.g. local grant, Opened unlocked door, Facility code grant etc.).



Event Type	Source	Definition
Video	Video	Video-related events, including: <ul style="list-style-type: none"> • Connection Loss • Motion Detected • 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**.
The Event Types Listing page is displayed.
2. From the Event Types Listing page, click **Add New Event Type**.
3. On the Event Type: Add New page, enter a name for the new event type.
4. Check the **Alarm** box if this event type will always generate an alarm.
5. Complete the remainder of the page with the required settings.
6. Click  to save the new event type.

Editing Event Types

1. Select  > **Event Types**.
The Event Types Listing page is displayed.
2. From the Event Types Listing page, 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 Defined Fields - Introduction

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 46.

User Defined Fields - Adding a Field

User defined fields are used to collect additional details about users on the Identities page. After you add all the fields that you need, you will need to add at least one tab to display the new fields. For more information, see *User Defined Fields - Adding User Defined Tabs* below.

1. Select  > **User Fields**.

The User Defined Fields Listing page displays.

2. Click **Add New User Defined Field**.

The User Defined Field: Add New screen displays.

3. Give the new field a name in the **Name** field.
4. Select the field **Type**.

The options are:

- **String** — the field supports words and numbers.
- **Integer** — the field supports numbers only.
- **Boolean** — the field is a check box. The system interprets the Boolean field as a Yes or No question. When you use the field, check the box to indicate "yes" and clear the box to indicate "no".
- **Date** — the field supports a date only. When you use the field, click the field to display a calendar then select a date.

5. Click  to save the new field.

NOTE: User defined fields cannot be edited, only deleted.

NOTE: When searching for identities using user defined fields there may be issues with string and integer fields. Searches will identify exact matches, but may not operate correctly for 'not equal to' searches. In order to correct this issue, create an Identity Profile including all relevant identities then complete a Batch Update.

User Defined Fields - Adding User Defined Tabs


To use user defined fields, you must add a new tab to host the fields before the fields can be used on the Identities page. It is recommended that you add tabs after you've added all the fields that you need.

1. Select  > **User Fields**.


The User Fields Listing page is displayed.

2. From the User Fields Listing page, click the **Tabs** tab.
3. Click **Add New User Defined Tab**.


The User Defined Tab: Add New page displays.


4. Enter a name for this new tab then click .

The page refreshes to show a list of all the user defined fields that have been configured in the system.

5. From the Available list, select all the fields that should be displayed on the page, then click .

The field is added to the Members list to show that it is now part of the page.


To remove a field from the tab, select the field from the Members list and click .

6. Click  to save your changes.

User Defined Fields - Editing User Defined Tabs




1. Select  > **User Fields**.


The User Fields Listing page is displayed.

2. From the User Fields Listing page, 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 - Introduction



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.

User Lists - Adding Items to a List

NOTE: Any changes you make to the lists are automatically included in identity related collaborations.

1. Select  > **User Lists**.

The User Defined Lists Listing page is displayed.
2. On the User Defined Lists Listing page, 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 then click .
- The new value is added to the Current Values list.
4. Repeat the previous step until all the new values you want are listed.
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 Listing page is displayed.

2. On the User Defined Lists Listing page, 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 Listing page is displayed.


2. On the User Defined Lists Listing page, 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

When you select  > **System Settings**, you can set your system preferences and configure remote access to the Access Control Manager system from external domains.




System Settings - General page







In the top-right, select  > **System Setting** to display the System Settings General page.



This page allows you to set custom system-wide default values.

Be aware that certain user specific settings configured in the **My Accounts** page will override the settings on this page.

Feature	Description
Enhanced Access Level	Check this box to 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 cardholders 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 cardholder. After you enable duplicate PINs, the available Door Mode options are:

Feature	Description
	<ul style="list-style-type: none"> • Card Only — This door can be accessed using a card. No PIN is required. • Card and Pin — This door can only be accessed using both a card and a PIN. • Facility Code Only — This door can be accessed using a facility code. <p>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.</p> <p>Do the following before allowing duplicate PINs to ensure that no doors are in either PIN Only or Card or PIN door modes:</p> <ol style="list-style-type: none"> 1. Select Physical Access > Doors to navigate to the Door Listing page. 2. For each door currently in either PIN only, or Card or PIN mode: <ul style="list-style-type: none"> • Select the check box beside the door. • Either select Door Action > Restore to restore to the configured door mode or select an alternative mode from the Door Mode dropdown list. <p>To allow duplicate PINs, check this box then:</p> <ul style="list-style-type: none"> • Click OK when the message 'Enabling duplicate PINs is an irreversible setting and cannot be undone. Are you sure you want to continue?' displays. • Click OK when the message 'Proceed with enabling duplicate PINs?' displays. <p>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.</p>
Badge Template Photo Height	<p>Enter a new value in pixels to change the default height for displaying the ID photo used for badge templates on the screen then click .</p> <p>The default value of 153 px is approximately 1½ inches or 3.5 centimeters.</p>
Badge Template Photo Width	<p>Enter a value in pixels to change the default width for displaying the ID photo used for badge templates on the screen then click .</p> <p>The default value of 117 px is approximately 1 inch or 2.5 centimeters.</p>
Identity Auto Increment Field	<p>Check this box to enable the system to automatically increments the read-only Sequence Number field on the Identity page.</p> <p>This option is disabled by default.</p> <p>NOTE: The system will only apply this setting to new identities.</p>
Identity Auto Increment Start	<p>If you enabled Identity Auto Increment, enter the number the system will start counting from then click .</p> <p>The default value is 1.</p>

Feature	Description
	NOTE: The system will only apply this setting to new identities.
Identity Auto Increment Step	<p>If you enabled Identity Auto Increment, enter the value the system uses to increment the sequence number then click .</p> <p>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.).</p> <p>NOTE: The system will only apply this setting to new identities.</p>
Language	<p>Select a language that the system will display by default.</p> <p>Each user with access to the Access Control Manager system will be able to set their own language preferences from the My Account page.</p> <p>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.</p>
Maximum Active Tokens	Enter the maximum number of tokens that can be active per identity then click  .
Maximum Login Attempts	<p>Enter the maximum number of attempts a user has to log into the Access Control Manager system before they are locked out, then click .</p> <p>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.</p> <p>The default value is 5.</p>
Password Strength Enforced	Check this box to enable a minimum password strength requirement. Weak passwords (less than four characters) are not accepted.
Post Roll	Enter the number of seconds a camera continues to record after a recorded video event.
Pre Roll	Enter the number of seconds of video that is automatically added before a recorded video event.
Private Message	Enter a short message to display on the log in screen.
Show Identity Photos	Check this box to enable a photo to be displayed beside each identity reference.
System Message	<p>Enter a title you want to use for the system then click .</p> <p>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.</p>
System Support	<p>Enter the contact details of your Avigilon support representative then click .</p> <p>This information is displayed when a user clicks Support.</p>
Token Expiration Time	Enter the default number of days before a token expires then click  .

Feature	Description
Use/Lose Threshold	Enter the default number of days a token can be unused before it is automatically deactivated, and then click  .
Video Windows Count	Enter the maximum number of video display windows that can be open at the same time, then click  .
Create New Report	Click this button to generate a PDF of the values on this page.

Remote Authentication from External Domains

Remote authentication allows you to configure the Access Control Manager appliance to use an external domain server to authenticate users that need access to the system, or to secure an LDAP Identity pull collaboration type. Either of these allows users to use their local domain username and passwords to access the system, and will not need a separate password configured in the ACM appliance. However, user access permissions are still based on the roles they are assigned within the ACM appliance.

To use remote authentication, you need to:

- Add one or more external domains
- Add one or more AD or LDAP servers to each domain to the system
- Enable each remote host to present its SSL certificate on connection to the ACM server software
- Enable remote authentication in the ACM appliance

SSL certificates are used to verify remote hosts and to encrypt all traffic between connected hosts.

Certificates can be recognized in two ways:

- 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.
- 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.

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 choose one of these domains to use for authentication. This is done on the configuration screen for the given Identity.

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.

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.

System Settings - Configuring Remote Authentication Using SSL Certificates

SSL certificates can be trusted (or accepted) in two ways: as pinned certificates or fully trusted certificates.




Using Pinned Certificates

Requirements:

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:


- Configure a Windows domain controller. For an LDAP collaboration, TLS encryption must be activated.
- Obtain the fully-qualified domain name of the DNS server for remote server's domain.
- Enable AD Certificate Services.
- Create a root certificate and a Domain Controller Authentication certificate.


Once you have all the requirements, log in to the ACM appliance, 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 . The domain controller is added to the Current Servers list.
7. Click .

8. Select the **Remote Authentication** tab.

NOTE: The **Default Domain** and **Default Server** options are not required for remote authentication.

9. Select the **Validate Certificate** check box.
10. Click  .
11. Repeat the previous steps on each ACM appliance in your system that requires remote authentication.
12. 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?** check box in the Account Information area.
 - 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@avigilon.com
 - f. Click  .

Next time the user logs in to the ACM appliance, they use their ACM system login name and the password.







Using Trusted Certificates

Requirements:



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:

- Configure a Windows domain controller. For an LDAP collaboration, TLS encryption must be activated.
- Obtain the fully-qualified domain name of the DNS server for remote server's domain.
- Enable AD Certificate Services.
- Obtain a root certificate and a Domain Controller Authentication certificate.
- Export the Domain Controller's root CA certificate in Base-64 encoded X.509 (.CER) format. (Do not export the private key.)
- Change the export file extension from `.cer` to `.pem` before you upload the file to the appliance.

Once you have all the requirements, log in to the Access Control Manager appliance, and complete the following steps:

1. In the top-right, select  > **Appliance**.
2. Under the Appliance tab, enter the IP address of your domain's DNS server in the **Name Server** field.
3. Click .
4. In the top-right, select  > **System Settings**.
5. Select the **External Domains** tab.
6. Click **Add External Domain**.
7. On the External Domain: Add New page, enter a name for this external domain.
8. In the **Server** field, enter the full DNS name of your domain controller.
9. Click . The domain controller is added to the Current Servers list.
10. Click .
11. Select the **External Domains** tab to display the listing page.
12. Click **Certificates** (next to the Create New Report button).
13. On the following listing page, click **Add Certificates Listing**.
14. Click **Browse** then locate the domain controller CA certificate that you exported. Make sure the file extension has renamed to .pem.
15. Click .
16. Select the **Remote Authentication** tab.

NOTE: The **Default Domain** and **Default Server** options are not required for remote authentication.

17. Select the **Validate Certificates** check box.
18. Click .
19. Repeat the previous steps on each ACM appliance in your system that requires remote authentication.
20. 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?** check box in the Account Information area.
 - 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@avigilon.com
 - f. Click .

Next time the user logs in to the ACM appliance, they use their ACM login name and the password.



System Settings - Remote Authentication

When you select the **Remote Authentication** tab on the System Settings screen, the Remote Authentication page is displayed.

This page enables the ACM software to provide secure connections and encrypted traffic between servers and clients.


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.

It also allows you to define the default domain and server that hosts the Active Directory database that the system uses to authenticate users.

Feature	Description
Default Domain	Select a domain from the drop down list. 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. The default setting is not checked. Use the default setting only if you do not need to validate certificates from remote servers. 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.

Badge Templates and the Badge Designer

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. 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.

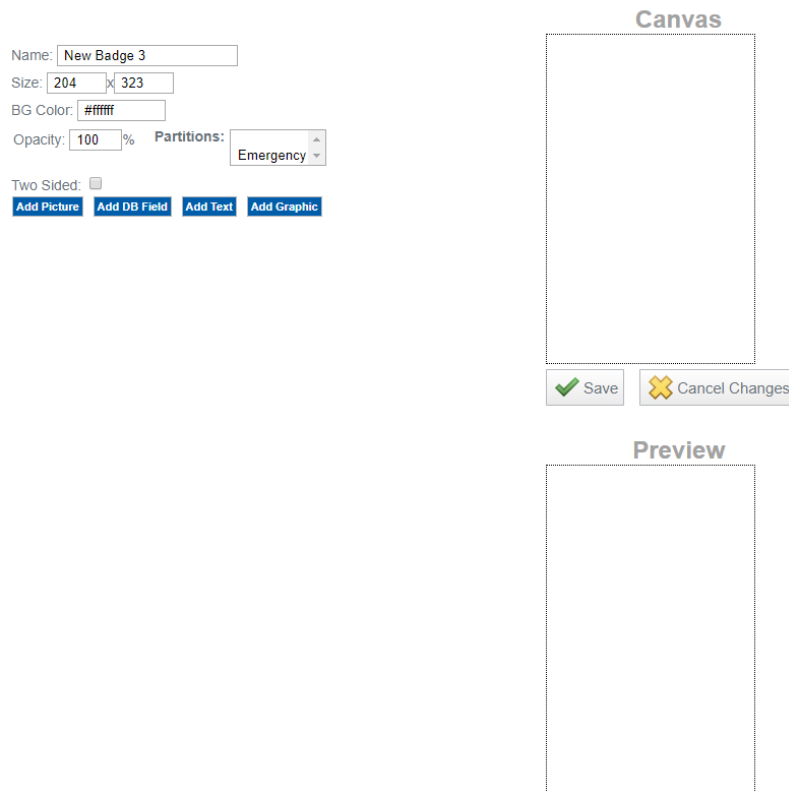
NOTE: Badge templates can be designed as either one- or two-sided. A two-sided badge must be printed by a badge printer possessing duplex (double-sided printing) capability.

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.



The screenshot shows the Badge Designer interface. On the left, there are configuration fields: 'Name' (New Badge 3), 'Size' (204 x 323), 'BG Color' (a color picker showing #ffffff), 'Opacity' (100%), and 'Partitions' (Emergency). Below these are buttons for 'Add Picture', 'Add DB Field', 'Add Text', and 'Add Graphic'. To the right, there is a large 'Canvas' area and a smaller 'Preview' area below it. At the bottom of the canvas area are 'Save' and 'Cancel Changes' buttons.

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** check box.

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* below and *Fields Common to Picture and Graphic Objects* on the next page.

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** check box 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* below 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. TYou can resize the object to ensure all text is visible as well as change the font, size, and color. Additionally, select the **Auto Resize** check box 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* below 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.
	1 is the lowest layer, 2 is in front of 1 and so on. You can reorder the layers by typing over the

Field	Description
	value for each object.
Location	<p>Click and drag the object on the canvas, or enter the horizontal and vertical coordinates of the top left corner.</p> <p>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.</p>
Dimensions	<p>Modify the default size of the object (in pixels) if needed.</p> <p>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.</p> <p>The first field is the width and the second field is the height.</p>
Rotation	<p>Select the number of degrees to rotate this object clockwise from the dropdown list.</p> <p>The default is 0 degrees.</p>

Fields Common to Data Field and Text Objects


Field	Description
BG Color	<p>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.</p> <p>Use the color picker to either select a color from the palette or manually enter the color in RGB, HSV or hex code format.</p>
Opacity	<p>Enter how opaque you want the background color to be, in conjunction with the layer order.</p> <p>0% is fully transparent and the default setting of 100% is fully opaque.</p>
Font	<p>Select the font you want for the text..</p> <p>The font list includes text fonts and barcode fonts. Text fonts are listed first, then barcode fonts.</p>
Font Size	Enter the font size in points. If Auto Resize is selected, this is the maximum font size.
Auto Resize	Select this check box 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	<p>Click this field to choose a font color.</p> <p>Use the color picker to either select a color from the palette or manually enter the color in RGB, HSV or hex code format.</p>
Opacity	<p>Enter how opaque you want the font color to be, in conjunction with the layer order.</p> <p>0% is fully transparent and the default setting of 100% is fully opaque.</p>

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.

Field	Description
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

- 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.
- 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**, etc. The font option list the text fonts first then the barcode fonts .
- 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 - listing page

When you select  > **Badge Designer**, the Badge Templates listing page 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	<p>The name of the badge template.</p> <p>Click the name to edit the badge template. For more information, see <i>Using the Badge Designer</i> on page 260.</p>
Commands	<p>Click  to delete the badge template.</p> <p>Click  to copy the badge template.</p> <p>The copy of the badge template is automatically added to the top of the list.</p>
Add Badge Template	Click this button to add a new badge template. For more information, see <i>Using the Badge Designer</i> on page 260.

External Systems - Introduction

The Access Control Manager system can connect and integrate with external systems to provide video or power backup support.

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.




External Systems - Adding

In order to add photos to the Identities database or record video for surveillance, you must first add cameras to the system.



NOTE: Before you can add a camera or video device, you must first connect a supported device to your network or server, then configure the device as described in your device user's guide. Make sure to write down the camera's IP address and onboard URL.

You can add individual cameras or you can add whole network video systems that can be configured to work with doors and events in the Access Control Manager system.

This procedure also applies to adding LifeSafety power supplies.



1. Select  > **External Systems**.
2. Select the tab for the external system you want to add.
3. From the External Systems listing page, click .
4. In the following page, complete the required fields to add the new external system.
5. Click  to save the new external system.

External Systems - Editing

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.

External Systems - Deleting

Deleting an external system does not remove it from your system, it will simply prevent the appliance from communicating with the external system. You may still need to uninstall the external system as required.

1. Select  > **External Systems**.
2. Select the tab for the type of external system you want to delete.
3. From the listing page, click  beside the system you want to 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. Examine the rights assigned to the preconfigured **ACC Administrator** delegation:
 - Appliance Listing
 - Delegations Listing
 - Door Grants
 - Doors Listing
 - Identities Listing
 - Identities Login - Remote
 - Identities Photo Render
 - Inputs Listing
 - Panels Listing
 - Partitions List
 - Roles Listing
 - Subpanels Listing
 - System Summary Listing
2. If additional rights are required, such as the Partitions right because your ACM installation is

partitioned and you want the ACC operator to access doors within the partitions, you must add these rights to this delegation, or create a new delegation with the rights assigned to the preconfigured **ACC Administrator** delegation.

3. 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
4. If you created a new delegation to use instead of the preconfigured **ACC Administrator** delegation, you also need to modify the preconfigured **ACC Administrator** role, or create a new role that allows the ACC software to communicate with the ACM system.
 - a. If you modify the preconfigured **ACC Administrator** role, under the role's **Delegate** tab, assign only the new delegation that was created to replace the preconfigured **ACC Administrator** delegation.
 - b. If you create a new role:
 - 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** check box and click **Save**.

Additional tabs will appear.
 - e. In the role's **Delegate** tab, assign only the 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.
5. If you plan to import Active Directory identities to the ACM appliance or the ACC software, configure an LDAP Collaboration. For Active Directory Remote Authentication, configure remote authentication from external domains.
6. 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.
- 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.
7. If your ACM appliance uses partitions, add the identity as a member of the partitions they will need to access from the ACC Client.

Once these settings are applied, an ACC Client can connect to the ACM appliance.

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.

NOTE: Images cannot be captured with a local camera from an ACM client running in the Internet Explorer or Safari web browsers, or running on a mobile device.
 - **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.

Bosch Intrusion Panels

The following procedures relate to Bosch intrusion panels.

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  .

Editing a Bosch Intrusion Panel

To edit/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/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**.

Synchronizing 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), then the panel will need to be re-synchronized to the ACM system. When the panel is out of synch then a warning message (Warning, ACM and the Intrusion Panel are not synchronized, go to Settings ->External Systems->Bosch Intrusion and resync) will display on the screens available under the **Monitor > Intrusion Status** menu path.

To synchronize a Bosch intrusion panel:

1. Select  > **External Systems**.
2. Click the **Bosch Intrusion** tab.
3. Either:
 - Click  at the top level to synchronize all panels that are currently out of synch.
 - Click  beside the panel name to synchronize an individual panel.

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/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 46.
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 Custom Functions: 1 Keypads: 4 Events: 127 Passcode Users (+1 Installer): 10 Points: 16 Programmable outputs: 3 RF Points: 8 SKED Events: 1 Firmware version: 3.0.2 or greater
B4512	Areas: 2 Custom Functions: 2 Keypads: 8 Events: 127

	Passcode Users (+1 Installer): 32 Points: 28 Programmable outputs: 27 RF Points: 20 SKED Events: 5 Firmware version: 3.0.2 or greater
B5512	Areas: 4 Custom Functions: 4 Keypads: 8 Events: 255 Passcode Users (+1 Installer): 50 Points: 48 Programmable outputs: 43 RF Points: 40 SKED Events: 5 Firmware version: 3.0.2 or greater
B6512	Areas: 6 Custom Functions: 6 Keypads: 8 Events: 1,000 Passcode Users (+1 Installer): 100 Points: 96 (8 on-board, 88 off-board and virtual) Programmable outputs: 3 RF Points: 88 SKED Events: 6 Firmware version: 3.0.2 or greater
B9512G	Areas: 32 Custom Functions: 32 Keypads: 32 Events: 10,192 Passcode Users (+1 Installer): 2,000

	Points: 599 Programmable outputs: 599 RF Points: 591 SKED Events: 80 Firmware version: 3.0.2 or greater
B8512G	Areas: 8 Custom Functions: 8 Keypads: 16 Events: 2,048 Passcode Users (+1 Installer): 500 Points: 99 Programmable outputs: 99 RF Points: 91 SKED Events: 40 Firmware version: 3.0.2 or greater
D9412GV4	Areas: 32 Custom Functions: 16 Keypads: 16 Events: 1,000 Passcode Users (+1 Installer): 999 Points: 246 Programmable outputs: 131 RF Points: 238 SKED Events: 40 Firmware version: Version 2.0 or greater
D7412GV4	Areas: 8 Custom Functions: 4 Keypads: 16 Events: 1,000 Passcode Users (+1 Installer): 399 Points: 75

Programmable outputs: 67
RF Points: 67
SKED Events: 40
Firmware version: Version 2.0 or greater

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 Avigilon Servers 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.
User ID Range	<p>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.</p> <p>Avigilon recommends that you:</p> <ul style="list-style-type: none"> • Reserve a block of numbers within this range dedicated for ViRDI biometric tokens for use by the ACM system. • Do not assign any of those numbers to physical cards for other types of access readers. • Do not modify this range. <p>NOTE: If you must modify the range, contact Avigilon customer support for guidance.</p>
Web Service Port	<p>Accept the default port or enter a new port number.</p> <p>If you change this port number from the default port (9875), you must also change the</p>

Feature	Description
	corresponding port number on every Biometric Enrollment (BE) Manager used for identity enrollment.
Partitions	<p>NOTE: If no partitions are defined for this system, this feature is not available.</p> <p>Select one or more partitions.</p> <p>Partitions allow you to define who can see or edit items in the system. If you do not select a partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system and that you are allowed to view appear in this list. You can only see the partitions that you are a member of.</p>
Delete	Click to delete the server from the system.
Update	Click this button to add the ViRDI server to the system.


Maps - Introduction

Maps are a graphical representation of your access control system. You can import any image of your facility into the Access Control Manager application then add doors, inputs, outputs, global actions, and camera shortcuts so that user access and events can be monitored in reference to where they occur.


Maps - Creating and Editing a Map

Maps can be used to 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, PDF, TIP and WMF format as the base of the map.

Maps are also used to display Mustering dashboard elements. For more information about setting up a Mustering dashboard, see *Mustering - Creating a Dashboard* on page 193.

1. Select  > **Maps**.
2. To add a new map, click **Add New Map Template**.
 - a. On the following Maps Template: Add New page, enter a name for the map.
 - b. Click **Browse** then locate the image file that you want to use for the map.

If you are planning to create a Mustering dashboard, select the **Use Blank Canvas** check box to use a blank background.
 - c. Enter the dimensions of the map in the **Re-Size To** fields.

NOTE: If you enter a size that matches the image's aspect ratio, the map image is re-sized accordingly. If you enter a size that does not match the image's aspect ratio, the system centers the image then crops the sides to match the defined setting.
 - d. Click  to save the new map template.

The page refreshes and displays the Map Template: Edit page.
3. To edit a map, click the name of a map template. The Map Template: Edit page is displayed.




4. In the Map Details area, click **Add** beside each item that you want to add to the map.

An icon that represents the new item is automatically added to the top left corner of the map and new options are displayed.



- a. Move the icon to the appropriate location on the map.



Tip: As you add more items, each icon is automatically added to the top left corner of the map. It is recommended that you move each icon immediately to avoid losing track of each item.

- b. In the Map Details area, select what the icon represents. Only items that have been configured in the system are displayed in the drop down list.




5. Repeat the previous step until you've added all the items that are required.
6. To move an item on the map, click and drag the icon to the appropriate location.
7. To edit what an icon represents, locate the item in the Map Details list and select a new option from the appropriate drop down list.
8. To delete an item from the map, click  beside the item in the Map Details area.
9. Click  to save your changes. It is recommended that you save frequently. Saving also causes the page to refresh, so any changes have not been updated in the preview may appear after you save.
10. Click  to return to the Map Templates Listing page.




Maps - Linking Maps



You have the option of linking your maps together to provide different views and different levels of detail of the same area. After you create each map, you can link them together by using the  **Zoom In** or  **Zoom Out** option to define how the maps are linked together.

For example, say an operator has detected an alarm in a building. His monitor displays the building's map, showing the alarmed point, but he needs to get a closer look to confirm the exact position of the alarm. To do this, he clicks  which is linked to a floor view. The floor view map appears with a closer view of the alarmed point. Once he has taken care of the alarm, he can then click  to return to the general building map and resume general surveillance.

Complete the following steps to link maps together:

1. Select  > **Maps**.
2. Create a map for each view that you want of your facility. For more information, see *Maps - Creating and Editing a Map* on the previous page.
3. From the Map Template Listing page, click the name of the map with the widest view of the facility.
4. On the Map Template Edit page, click **Add** beside the Zoom In option in the Map Details area.
5. In the following drop down list, select the map with the close-up view of the facility.
6. From the top left corner of the map, move the  icon to the area that the linked map represents.
7. Click  to save your changes.

8. Click  to return to the Map Template Listing page.
9. Click the name of the next map.
Select the map that you just linked to on the previous map.
10. On the Map Template Edit page, click **Add** beside the Zoom Out option in the Map Details area.
11. In the following drop down list, select the first map that you added a link from. Now the two maps are linked back together.
12. From the top left corner of the map, move the  icon to the edge of the map to show where the linked map expands from.
13. Click  to save your changes.
14. Repeat the previous steps until all your maps are linked together in a logical order.

Always use the  **Zoom In** icon to link a map with less detail (such as a building or campus) to a map with more detail (like a floor or room). The  **Zoom Out** icon is meant to link a detailed map to a wider, less detailed map.

Use this procedure to create a series of links that progressively bore down to greater and greater granularity, or telescope up to provide a larger view.






Using a Map

After a map has been configured, access it from the Monitor page and use it as a quick visual reference to all the items that may be installed in a facility.

From the map, you can:

- Monitor the status of hardware items: doors, panels, subpanels, inputs and outputs.
- Control doors.
- Keep track of identities as they arrive at muster stations from the Mustering dashboard.

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

-  : A green bar indicates the hardware item is operating normally.
-  : A red square indicates the hardware item is in an alarm state. The counter in the square shows the number of unacknowledged events.
-  : A solid blue disk indicates an active override is in effect on the door. A hollow blue disk  indicates an inactive override is defined. For more information, see
-  : A red bounding box is displayed around the status bar of a door in Priority Mode.









To access and monitor your site from a map:


1. Select **Monitor > Maps**. The Map Templates page displays.
2. In the Map Templates Listing page, click the name of a map.

The map is displayed. Some of the displayed elements may not appear in your map or the example below.






Figure 18: Example map

Feature	Map Icon
Doors	
Panels	
Subpanels	
Inputs	
Outputs	
Cameras	
Zoom In	
Zoom Out	

Feature	Map Icon
Global Actions	
Dashboard Elements	Square, circle or text object

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

To...	Do this...
Review hardware status	<p>The colored bar below each item displays an overview of the current communication and power status. Click the icon on the map to display the control menu.</p> <p>For more information about the colored hardware status bar, see the specific hardware status page.</p> <p>For more information about the status colors, see <i>Status Colors</i> on page 37.</p>
Review an alarm	<p>If you see a red alarm indicator, the item on the map is in an alarm state. Click the alarm indicator to see the status details.</p> <p>For more information about alarm actions, see <i>Monitor Alarms</i> on page 24.</p>
Modify or delete an override	<p>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. Click the indicator to open the <i>Doors: Overrides</i> page to see details.</p>
Respond to a priority situation	<p>If you see a red bounding box around the status indicator, the door is in Priority Mode.</p> <p>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.</p>
Display video	<p>Click the  on the map to display the Camera Video window.</p>
Open a linked map	<p>Click  to display a linked map, or  to display a linked map.</p>
Monitor the dashboard	<p>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.</p> <p>The dashboard displays the number of identities in the area and may include the name of the area. In <i>Example map</i> on the previous page, the dashboard is the gray square.</p> <p>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.</p>

Priority Situations

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 VertX® panels. If you only have 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 VertX® and Mercury doors, do not include VertX® doors in any group of doors that are associated to your Priority Door Policies or Priority Door Global Actions.

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 Operators, 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.



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 289

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 policies 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 290. 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 Operators 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 291.

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 Operators .

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 than 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 for 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. Login as the Priority ACM Operator.
3. Activate the Priority Door Policy:
 1. Navigate to the priority map.
 2. 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. Login as the Priority ACM Operator.
 7. Deactivate the Priority Door Policy:
 1. Navigate to the priority map.
 2. 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	
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	
	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		
	Non-priority Door Policy		
	Non-priority Door Global Action		
	Macro/Trigger		
	Base Mode		
	Job Specification (two global actions)		
	Door template		

Overriding Door Modes and Schedules

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.

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.

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 291. 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.

An override starts and ends at the beginning of the minute of its scheduled time. Therefore it always overlaps or matches the start or end time of a regular schedule or override when the end time of one is the same as the start time of the other, or vice versa.

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 Listing page, 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**.

The Door Listing page is displayed.

2. Click the check box 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**.

The Override dialog box is displayed.

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.
 - **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. The override begins and ends at the beginning of the minute you specify.

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 279.

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 .

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.
 - **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. The override begins and ends at the beginning of the minute you specify.

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  .


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 into the system, you can choose to change your password any time from the My Account page.

1. In the top-right, select  > **My Account**.
2. On the following Profile page, enter your current password in the **Old Password** field.
3. In the **Password** field, 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 four characters long.

4. Click  to save your new password.

A system message tells you that you will be logged out.

5. When the login screen appears, log in with your new password.

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 Listing page, 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 check box 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** check box 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 Updatebatch job to apply a new, updated or temporary identity profile to all of the identities in a predefined group.

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 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 check box 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

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 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 check box 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 check box 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.

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 **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** check box 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 check box 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
View the intrusion status	Monitor Intrusion Panel Status
Control the assigned intrusion panels	Intrusion Panel Master Instant Arm

Permissions	Rights
	Intrusion Panel Master Delay Arm
	Intrusion Panel Master Force Instant Arm
	Intrusion Panel Master Force Delay Arm
	Intrusion Panel Perimeter Instant Arm
	Intrusion Panel Perimeter Delay Arm
	Intrusion Panel Perimeter Force Instant Arm
	Intrusion Panel Perimeter Force Delay Arm
	Intrusion Panel Away Arm
	Intrusion Panel Force Away Arm
	Intrusion Panel Disarm
	Intrusion Panel Silence
	Intrusion Point Bypass
	Intrusion Point Unbypass
	Intrusion Output Activate
	Intrusion Output Deactivate
View live and recorded video	Cameras Show
	Cameras Login
	Monitor Cameras Show Video
Add new identities. Cannot update fields after initial identity setup	Identities My Account
	Identities Listing
	Identities Show
	Identities Advance Search
	Identities Date Search
	Identity Profiles Listing
	Identity Profiles Show List
	Identities New
	Identities Create

Permissions	Rights
	Identities Edit
	Identity Profiles Populate Values
	Identities Custom Layout Save
Add, modify, and update available roles	Identities Roles List
	Identities Roles Update
Add, modify, and update tokens	Tokens Listing
	Tokens Show
	Tokens New
	Tokens Create
	Tokens Edit
	Tokens Update
	Tokens Set Free Pass
	Identity Profiles Tokens Listing
Add and modify groups	Identities Groups List
	Identities Groups Update
View assigned access permissions	Identities Show Access
	Identity Profiles Show Access
Capture live photos and save	Identities Image Capture
	Identities Image Save
	Identities Code Image
	Identities Photo Capture
Add and upload photos	Identities Photo Edit
	Identities Photo Update
	Identities Photo Render
	Identities Upload Photo
View transactional data	Identities Transactions
Print and issue badges	Identities Badge Show
	Identities Badge Screen
	Identities Print Badge

Permissions	Rights
	Identities Badge Render
	Identities Update Badge Preview
	Identities Update Badge
Perform REST actions	Identities Photo List REST
	Identities Photo Show REST
	Identities Photo Create REST
	Identities Photo Update REST
	Identities Photo Delete REST
	Appliance REST Generation Transaction
View Identity Policies	Identities Policies Show
	Identities Policies Listing
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

Permissions	Rights
	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
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
Add and modify Doors	Doors New
	Doors Edit
	Doors Create
	Doors Update
	Doors New/Edit Appliance Change
	Doors New/Edit Manuf Change

Permissions**Rights**

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

Doors Cmacro Type Change

Doors Cmacro Op Type Change

Permissions**Rights**

	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
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

Permissions	Rights
	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
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

Permissions	Rights
	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
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

Permissions	Rights
	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
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

Permissions	Rights
Edit Global Linkages	Global Linkage Show
	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
Delete Global Linkages	Global Linkage Remote Execute
	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
View Delegations	Delegations Listing
	Delegations Show
View Partitions	Partitions List
	Partitions Show

Permissions	Rights
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 Assign Ports Roles Assign Groups
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
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

Permissions	Rights
Add and modify Access Groups	Access Groups New Access Groups Edit Access Groups Create Access Groups Update Access Groups Door Assign
Add and modify Delegations	Delegations Edit
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
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

Permissions**Rights**

Add and modify Appliances

Appliance Software Listing
Appliance Virtual Port List
Appliance Software View Log
Appliance Backup Listing
Appliance Backup Show
Appliance Status Display
Appliance Log Show
Appliance Backup Directory List

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

Permissions	Rights
	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
	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

Permissions	Rights
	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
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

Permissions	Rights
Delete User Fields and User Lists	User Lists Update
	User Defined Tabs Delete
View System Settings	User Defined Tabs Delete
	External Domains Show
	External Domains Index
Add and modify System Settings	System Settings Index
	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
	External Domains Destroy
Delete System Settings	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

Permissions	Rights
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
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

Permissions	Rights
	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
	Intrusion Panel New
	Intrusion Panel Create
	Intrusion Panel Edit
	Intrusion Panel Update
	Intrusion Panel Detail Update
Delete External Systems	Image Devices Delete
	Exacq Server Delete
	External Systems Delete
	Avigilon Server Remove
	Salient Server Delete
	Milestone Server Delete
View Maps	Maps Listing
	Maps Show

Permissions	Rights
Add and modify Maps	Maps New Maps Edit Maps Create Maps Update Maps Edit and Add Detail
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

Create, edit, and delete batch jobs and job specifications

Rights

Batch Job Specification Edit
Batch Job Specification Activate
Batch Job Specification PostProcess
Batch Job Specification
JobSpecificationList
Batch Job Specification Create
Batch Job Specification Update
Batch Job Create
Batch Job New
Batch Job Update
Batch Job List
Batch Job Output
Custom Report Schedule
Reset Custom UI Settings
System Settings Localize
Batch Job Specification Destroy
Batch Job Destroy